GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Performance Oversight Pre-Hearing Responses

Dr. Christopher Rodriguez

Submission to

Committee on the Judiciary and Public Safety
Chairperson Charles Allen
Council Member, Ward 6

February 25, 2021

Committee on the Judiciary and Public Safety
John A. Wilson Building
1350 Pennsylvania Ave., NW, Suite 123
Washington, DC 20004

1. **Please provide a current organizational chart for the agency, including the number of vacant, frozen, and filled positions in each division or subdivision. Include the names and titles of all senior personnel and note the date the information was collected on the chart.**

Please see attachment "Q1 HSEMA" for the current organizational chart.

   a. **Please provide an explanation of the roles and responsibilities of each division and subdivision.**

Director's Office:
Provides executive leadership and administrative authority over HSEMA.

Chief of Staff:
Manages HSEMA's day-to-day enterprise activities and Administrative Division. Key personnel and functions include:

- Chief Administrative Officer: Manages HSEMA's day-to-day administrative functions.
- Grants Bureau: Manages the federal homeland security grant programs awarded to the District and the National Capital Region.
- Finance Bureau: Manages HSEMA's finances in accordance with District policies and priorities.
- Information Technology (IT) Bureau: Manages, in coordination with OCTO, HSEMA's IT systems and other technology needs.
- Human Resources Bureau: Manages, in coordination with DCHR, the recruitment and hiring of new HSEMA staff and contractors. Manages personnel issues across the agency.

Office of Public Affairs:
Manages external and internal communications as well as the legislative and policy initiatives for HSEMA.

Office of Legal Affairs:
Provides legal counsel and policy advice to the HSEMA director. Supports the work of the Homeland Security Commission.

Resilience and Emergency Preparedness Division:
Manages HSEMA's resilience and emergency preparedness activities. Key personnel and elements include:

- Chief of Resilience and Emergency Preparedness: Oversees the daily activities of the Resilience and Emergency Preparedness Division.
- Emergency Preparedness Bureau: Provides training and exercise opportunities to the District. Develops the District's corrective action program. Creates planning products to meet the needs of HSEMA and key stakeholders within the District. Provides regional and sub-

regional expertise to enhance preparedness capabilities, programs and initiatives in the National Capital Region (NCR).

- Resilience Bureau: Manages the District's long-term recovery program. Administers and oversees the District's Hazard Mitigation Program. Within this Bureau, the Disability Integration Coordinator ensures the District's emergency management program effectively meets the needs of people with disabilities and those with access and functional needs.

National Capital Region Threat Intelligence Consortium (NTIC):
Manages HSEMA's homeland security and intelligence activities. Key Personnel and elements include:

- Cyber Security Bureau: Collects, analyzes, responds to, and disseminates timely cyber threat information to and among the federal, state, local, and private sector agencies within the National Capital Region (NCR).
- NCR Watch/IC3 Bureau: Provides around-the-clock alert notifications and develops a common operating picture supporting coordination and collaboration on emerging incidents across the NCR.
- Public Safety Bureau: Focuses on unclassified production related to terrorism, crime, and public health for the public.
- National Security Bureau: Focuses on maintaining the baseline capabilities of the fusion center and providing support to law enforcement, first responder, and critical infrastructure partners.

Operations Division:
Manages HSEMA's steady-state and emergency operations activities. Key personnel and elements include:

- Chief of Operations: Oversees the Operation Division's daily activities.
- Emergency Operations Center (EOC) Bureau: Manages the District's Emergency Operation Center, oversees the District's Qualifications System, and processes EMAC requests.
- The Interoperable Bureau: Focuses on activities and programs that support response operations across the District emergency management enterprise. This includes three areas: interoperable communications, geospatial information systems, and unmanned aerial systems.
- Response Readiness and Coordination Bureau: Focuses on ensuring that the District enterprise is prepared for incident management and response operations. This includes responding to smaller, routine incidents – such as residential displacements, utility systems failures at government facilities, and transportation and utility emergencies throughout the District. This team coordinates the interagency response from notification of the incident through resolution, a process that can take weeks or months.
- Joint All Hazards Operation Center (JAHOC) Bureau: As the District's watch center, the JAHOC maintains 24/7 coverage of the District. Provides situational awareness of and coordinates resource requests for security and other incidents within DC.

- Facility and Security Bureau: Manages building and personnel security, access to Agency facilities, HSEMA's vehicle fleet, and the Agency's warehouse.

b. **Please provide a narrative explanation of any changes to the organizational chart made during the previous year.**

In January 2020, the District's Chief Resiliency Officer (CRO) moved from OCA to HSEMA to lead the Resilience and Emergency Preparedness Division. That Division, previously named the Homeland Security and Preparedness Division, focuses on resilience and emergency preparedness, allowing for the District's CRO to continue to build capacity and merge resilience with HSEMA's hazard mitigation portfolio.

2. **Please provide a current Schedule A for the agency which identifies each filled, vacant, unfunded, and funded position by program and activity, with the employee's name (if filled), title/position, salary, fringe benefits, and length of time with the agency (if filled). Please note the date the information was collected. The Schedule A should also indicate if the position is continuing/term/temporary/contract or if it is vacant or frozen. Please separate salary and fringe and indicate whether the position must be filled to comply with federal or local law.**

Please see attachment "Q2 HSEMA" for Schedule A.

3. **Please list all employees detailed to or from your agency during FY20 and FY21, to date. For each employee identified, please provide the name of the agency the employee is detailed to or from, the reason for the detail, the date of the detail, and the employee's projected date of return.**

During FY20 HSEMA had one employee detailed to another agency. Nicole Peckumn was detailed to the Mayor's Office of Public Affairs from February 11, 2019 to September 19, 2020. In addition, HSEMA had two employees detailed from another agency: (1) Daniel McCoy was detailed from the Department of Consumer and Regulatory Affairs from April 7, 2020 to July 5, 2020 and (2) Nickesha Collington was detailed from the Department of Human Resources from April 14, 2020 to August 11, 2020. All details to and from the agency were done for the good of the District, to improve performance, and to help meet the immediate needs of the District government.

4. **Please provide the Committee with:**

   a. **A list of all vehicles owned, leased, or otherwise used by the agency and to whom the vehicle is assigned, as well as a description of all vehicle collisions involving the agency's vehicles in FY20 and FY21, to date; and**

Please attachment "Q4 HSEMA" for a list of vehicles.

The accidents in FY20 and FY21, to date, involved the following:

- 6/5/20 – A u turn was being made by one driver as the other was backing up.
- 4/20/20 – Both drivers stated they did not know how the accident occurred.

b. A list of travel expenses, arranged by employee for FY20 and FY21, to date, including the justification for travel.

Name	Destination	Justification	Travel Period	Expense
Bradley, Nickea	State College, PA	State NFIP Coordinator/State Hazard	11/19/2019 - 11/21/2019	$348.00
DelGizzi, Jesse	Alexandria, VA	National Fusion Center Association	11/4/2019 - 11/7/2019	$161.40
DelGizzi, Jesse	Houston, TX	World Series Deployment	10/21/2019 – 10/24/2019	$1,844.26
DelGizzi, Jesse	Suffolk, NY	Digital Forensic Analysis Course	12/16/19 – 12/19/19	$901.31
DelGizzi, Jesse	Plain Dealing, LA	Basic Digital Forensic Analysis course	02/24/2020 – 02/27/2020	$1,626.58
Ehlman, Sarah	San Antonio, TX	2020 Preparedness Summit	03/31/2020 – 4/03/2020	$2,106.11
Gabry, Matthew	Houston, TX	World Series Deployment	10/21/2019 - 10/24/2019	$1,900.82
George, Margaret	Montgomery, Alabama	5th annual Fusion Center Human Trafficking Analysts' Training Event	02/25/2020 – 02/27/2020	$1,149.36
Gross, Travis	Kansas City, MS	Big City Emerging Leaders Program	01/13/2020 – 01/17/2020	$1,607.22
Harvin, Donell	Houston, TX	World Series Deployment	10/22/2019 - 10/24/2019	$434.50
Harvin, Donell	Sacramento, CA	State Threat Assessment Fusion Center	12/14/2019 – 12/18/2019	$1,471.00
Hewett, Megan	Houston, TX	World Series Deployment	10/21/2019 – 10/24/2019	$2,268.69
Huggins, Briana	Philadelphia, PA	FEMA Workshop	12/3/2019 - 12/5/2019	$716.30
Marcenelle, M.	San Francisco, CA	State Threat Assessment Fusion Center	12/15/2019 – 12/18/2019	$714.02
Mazzeo, Krista	Sacramento, CA	State Threat Assessment Fusion Center	10/2/2019 - 10/4/2019	$863.21
Mazzeo, Krista	Houston, TX	World Series Deployment	10/21/2019 - 10/24/2019	$2,418.03
Mazzeo, Krista	Alexandria, VA	NFCA Conference	11/4/2019 - 11/7/2019	$157.96
Mudambo, Mildred	Philadelphia, PA	2019 FEMA Region III Grants recipient	12/2/2019 - 12/4/2019	$722.70
Partridge, Nathanial	Savannah, GA	IAEM Conference	11/16/2019 - 11/21/2019	$1,909.03

Name	Destination	Justification	Travel Period	Expense
Peckumn, Nicole	Nashville, TN	MGT 404- Sports/Event Incident	11/4/2019 - 11/6/2019	$1,445.32
Peri, David	Las Vegas, NV	Comprehensive Cybersecurity Defense Course	02/09/2020 – 02/13/2020	$661.66
Quarrelles, Jamie	Savannah, GA	2019 International Association of Emergency Managers Conference	11/15/2019 - 11/21/2019	$3,234.46
Rodriguez, Christopher	Sacramento, CA	CSTAC Meeting	10/2/2019 - 10/4/2019	$1,404.63
Rodriguez, Christopher	Milan, Italy	Critical Infrastructure Protection and Resilience Expo	10/14/2019 - 10/16/2019	$3,782.83
Scott, Mark	Savannah, GA	IAEM Conference	11/17/2019 - 11/20/2019	$1,288.68
Shackelford, Jerica	Savannah, GA	International Association of Emergency Managers (IAEM) 2019 Conference	11/17/2019 - 11/21/2019	$1,909.85
Speranza, Carrie	Savannah, GA	IAEM Annual Conference 2019	11/15/2019 - 11/21/2019	$2,090.35
Sumbeida, Muniru	Philadelphia, PA	2019 FEMA Region III Grants Recipient	12/2/2019 - 12/4/2019	$549.52
Valentine, Amanda	Philadelphia, PA	FEMA Region 3 Grant Recipient Workshop	12/2/2019 - 12/5/2019	$909.63

5. Please list all memoranda of understanding ("MOU") entered into by the agency in FY20 and FY21, to date, as well as any MOU currently in force. For each, indicate the date into which the MOU was entered and the termination date.

The chart below has information related to Urban Areas Security Initiative (UASI) and State Homeland Security Program (SHSP) Memoranda of Agreement for FY19 and FY20, to date (January 24, 2020).

Agency	Purpose	Date Entered	Date Terminated
DC Health	Patient Tracking	October 23, 2019	September 30, 2020
DC Health	Medical Reserve Corps	October 23, 2019	May 31, 2021
District of Columbia Department of Human Services	Mass Care Program Development	October 23, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	CBRNE Detection	October 9, 2019	September 30, 2020

Agency	Purpose	Date Entered	Date Terminated
District of Columbia Fire and Emergency Medical Services	Terrorism Liaison Officer Program, Planning, Training, and Exercise Support	October 9, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	License Plate Reader Program	October 9, 2019	September 30, 2021
District of Columbia Office of the Chief Medical Examiner	Fatality Management Continuity of Operations (COOP)	October 4, 2019	September 30, 2021
District of Columbia Office of Unified Communications	Radio Cache (NCRCIG)	October 9, 2019	September 30, 2021
District of Columbia Office of Unified Communications	CAD Information Sharing and Interoperability	October 4, 2019	September 30, 2021
District of Columbia Office of Unified Communications	Interoperable Communications Planning, Training, and Exercises	October 4, 2019	September 30, 2020
District of Columbia Office of Unified Communications	9-1-1 Wireless Call Routing Analytics	October 4, 2019	May 31, 2021
Serve DC	Volunteers and Donations Management	October 23, 2019	September 30, 2020
DC Health	Medical Supplies and Equipment Cache	October 23, 2019	September 30, 2020
District of Columbia Department of Energy and Environment	Hazardous Materials Emergency Response Enhancement	October 9, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Chemical Protective Equipment	October 9, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	NIMS Typed Team Training	October 23, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Triage Equipment	December 18, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Law Enforcement Information Systems	October 4, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Personal Protection Equipment and CBRN Response	December 27, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Virtual Terrorism Response Training	October 23, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Crisis Negotiation Squad Response Vehicle	December 27, 2019	September 30, 2020

Agency	Purpose	Date Entered	Date Terminated
District of Columbia Public Schools	Emergency Response Information Portal (ERIP)	December 18, 2019	September 30, 2020
Serve DC	Citizen Preparedness and Volunteer Management	October 9, 2019	September 30, 2020
District of Columbia Office of Unified Communications	CAD Information Sharing and Interoperability (Continuation)	October 16, 2018	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Tactical Medical Casualty Care (TECC) Train the Trainer (CCA)	June 11, 2019	March 31, 2020
DC Health	Medical Reserve Corps (Continuation) (DCERS)	September 27, 2018	May 31, 2020
District of Columbia Metropolitan Police Department	License Plate Reader Program (Continuation)	September 27, 2018	September 30, 2020
District of Columbia Office of Unified Communications	Radio Cache - District of Columbia (Continuation)	September 27, 2018	September 30, 2020
District of Columbia Metropolitan Police Department	Law Enforcement Homeland Security Capabilities (Continuation)	September 27, 2018	January 31, 2020

6. Please list the ways, other than MOU, in which the agency collaborated with analogous agencies in other jurisdictions, with federal agencies, or with non-governmental organizations in FY20 and FY21, to date.

HSEMA participates on all of the National Capital Region Regional Emergency Support Function (RESF) committees of the Metropolitan Washington Council of Governments (MWCOG), as well as the Homeland Security Executive Committee (HSEC), the HSEC Advisory Council, HSEC Cyber Working Group, HSEC Fusion Center Working Group, the Complex Coordinated Attack (CCA) Working Group, and the Interoperability Working Group. HSEMA assigns personnel to support the NCR Preparedness System; co-chairing the NCR Critical Infrastructure Protection Workgroup and conducting a Federal Emergency Management Agency (FEMA)-funded project to develop an emergency food and water plan for catastrophic events. The Resilience Bureau collaborates with the U.S. Department of Homeland Security (USDHS) through membership on the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), to conduct two supply chain resilience studies for the District by USDHS/CISA (Cybersecurity and Infrastructure Security Agency) in partnership with other NCR jurisdictions. HSEMA collaborates with the FEMA Office of the National Capital Region and Coordination on multiple preparedness and operational issues. The Resilience Bureau Hazard Mitigation Program collaborates quarterly with FEMA Region III and other FEMA Region States (MD, VA, WV, PA, DE).

HSEMA works with the Disability Community Advisory Group (DCAG), a disability affiliated organization, to ensure our plans incorporate the needs of individuals with disabilities. HSEMA collaborates with the FEMA Region III National State Integration Coordinators and the National Capital Region Disability Integration Initiative Coordinators.

HSEMA collaborates with the U.S. Army Corps of Engineers (USACE) to conduct risk reduction operations regarding flood mitigation and assessments of emergency generator needs at District critical facilities.

Through HSEMA's Business Emergency Management Operations Center (DC BEMOC), District Government is building the resilience needed to minimize the devastation and ensure our neighborhoods can recover quickly. The DC BEMOC coordinates with the FEMA Region III business emergency operations centers, which cover much of the mid-Atlantic region. HSEMA meets monthly with the FEMA Region III Recovery Support Function Leadership Group (includes engagement of FEMA Region III states and relevant FEMA programs).

HSEMA's intelligence fusion center, the National Capital Region Threat Intelligence Consortium (NTIC), serves as the District's fusion center network to share information among federal, state, and local entities to maximize the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The NTIC collaborates with regional and federal entities daily through assigned liaisons. This includes joint intelligence products related to threat targeting to the District or in anticipation of large special events (i.e., 4th of July, State of the Union Address, and other large-scale events).

In 2019, after multiple mass shooting incidents around the globe, HSEMA partnered with the Mayor's Office of Religious Affairs (MORA) and the Metropolitan Police Department (MPD) to form the Interfaith Preparedness and Advisory Group (IPAG). This partnership provides support and solidarity to the District's places of worship prior to an emergency. The IPAG was provided emergency preparedness trainings and technical support with applications for federal funding to enhance security for their facilities. Additionally, HSEMA participates in several different working groups that bring together federal and local entities including the School Safety Alliance, DC's Human Trafficking Task Force, and IPAG.

HSEMA's Resilience Bureau collaborated with the Department of Energy and Environment (DOEE), Office of Planning, District of Columbia Public Schools (DCPS), and the Department of General Services (DGS) Protective Services Division (PSD) to enhance the District's flood mitigation. With DOEE, HSEMA provided technical assistance with floodplain and flood inundation mapping. The collaboration focused on project development for Flood Resiliency Strategies for Waterfront Southwest and Watts Branch, Climate ReadyDC, resiliency hubs, and emergency backup generators for critical facilities such as the Unified Communication Center and DC Water. With DCPS, HSEMA collaborated on the Safety Through Resiliency

Assessment Planning (STRAP) Pilot Assessments, River Terrace Education Campus (RTEC) emergency evacuation exercise, the Redbook Playbook, which provided a quick guide to the larger Redbook (DC Public Schools Safety and Emergency Plan), and School Safety Alliance migration to a more collaborative format. Also, with DGS-PSD, HSEMA collaborated for building assessments.

HSEMA is a member of the National Emergency Management Association (NEMA), allowing the agency to work directly with the analogous homeland security and emergency management agencies from every state and US territory. This allows the District to share resources during emergencies through the Emergency Management Assistance Compact (EMAC). This membership also allows the District to review and provide feedback on federal policy for disaster management and advocate for ongoing grant funding through NEMA's written comments and white papers.

HSEMA is a member of the National Governors Homeland Security Advisor Council (GHSAC). Like NEMA, GHSAC provides the agency with a forum to work with our homeland security and intelligence agency partners across the nation. It also allows the District to review and provide feedback on federal policy for homeland security and advocate for ongoing grant funding.

Nationally, HSEMA is a member of the Big City Emergency Managers (BCEM), which is a network of the most progressive emergency management agencies from the largest metropolitan areas around the country. Along with providing the District with another forum to formally advocate for disaster policy and funding, BCEM provides HSEMA with a method to collect and share best practices from peer agencies. The agency, especially our Division of Operations, regularly shares and receives plans, policies, and procedures from our counterparts to fill gaps in our doctrine.

HSEMA is a member of Silver Jackets Program supported by United States Army Corps of Engineers (USACE). Silver Jackets teams bring together multiple states, federal, and sometimes tribal and local agencies to learn from one another in reducing flood risk and other natural disasters. Shared knowledge is used to enhance response and recovery efforts when such events do occur. HSEMA collaborated with Silver Jackets on Flood Awareness Week, the Southwest and Buzzard Point Flood Resilience Strategy and the Watts Branch Flood Risk Management Study.

Regionally, the agency also participates as state representative on various FEMA committees and working groups, such as the Modeling and Data Working Group. HSEMA also participates in regular emergency response and recovery exercises across the region with our analogous local, state, and federal partners.

HSEMA administers the Statewide Interoperability Executive Council (SIEC), the mechanism through which the District manages public safety and emergency communications interoperability enhancement efforts. Under the District Statewide Communications Interoperability Plan, the SIEC provides policy-level direction to

District and regional partners on the development and maintenance of interoperable emergency communications. The SIEC oversees the Interoperable Communications Committee (ICC), a board made up of representatives from key SIEC agencies and other interested District, federal, and regional agencies. The Statewide Interoperability Coordinator serves as the liaison between the SIEC and ICC, while also coordinating and overseeing interoperability policy and procedures.

HSEMA also participates on or co-chairs several subcommittees for the National Special Security Events (NSSE) planning team. HSEMA regularly attends and participates at the meetings of the following associations: Hotel Association of Washington DC – Security Directors, Apartment Office Building Association – Emergency Preparedness Committee, the Consortium of University Police Chiefs, National Fusion Center Association Cyber Intelligence Network, Railway Alert Network, Amtrak Rail and Information Sharing Group, the Association of Metropolitan Water Agencies, Mid-Atlantic First Financial Sector, U.S. Department of Homeland Security – Sector Specific - Food and Agriculture Subcommittee, Maryland Center for School Safety Statewide School Safety Weekly Conference Call, the DC Venue Group, the Washington Nationals Security, and the Capital One Center Security. HSEMA also serves as a member of InfraGuard, the Washington-Baltimore High Intensity Drug Trafficking Area Program, and the Joint Force Headquarters-National Capital Region Joint Operations Information Group.

In accordance with Mayor's Order 2018-084 dated October 22, 2018, HSEMA is the chair and coordinating agency for the Mayor's Unmanned Aerial Systems (UAS) working group, which consist of representatives from District agencies and is tasked with evaluating and making recommendations for a comprehensive program to incorporate UAS in the District's airspace.

Finally, HSEMA partners daily with the American Red Cross (ARC) for emergency response. The ARC's National Capital Region Chapter operates under the ARC national charter and provides direct assistance to residents that require housing and incidental expenses following residential fires. HSEMA serves as the ARC's primary point of contact within the District.

7. For FY20 and FY21, to date, please list all intra-District transfers to or from the agency and include a narrative description of the purpose of each transfer.

FY 2020

FROM	SELLING AGENCY	DESCRIPTION OF SERVICES PROVIDED	AMOUNT
HSEMA	DCHR	Compliance Services	$12,500
HSEMA	DCHR	Employee Screening	$873

HSEMA	Office of Disability Rights	Sign Language Services	$89,159
HSEMA	DGS	EOC Assessment	$102,375
HSEMA	Office of Finance Resource Management	Agency Purchase Cards	$210,563
HSEMA	OCTO	Social Media Web Based Application	$200,000
HSEMA	OFOS	Single Audit	$6,646
HSEMA	Office of Finance Resource Management	RTS	$10,000
HSEMA	OCTO	FY20 IT Assessments	$110,125
HSEMA	Office of the Secretary	Records Retention	$3,600
HSEMA	DPW	Fleet Maintenance	$42.733
HSEMA	OUC	Radio Services	$6,647
HSEMA	DOEE	District Mitigation Plan	$108,628

FY 2021, to date (02/12/2020)

FROM	SELLING AGENCY	DESCRIPTION OF SERVICES PROVIDED	AMOUNT
HSEMA	Office of Finance Resource Management	RTS Cost	$10,000
HSEMA	DPW	Fleet Maintenance	$36,602
HSEMA	OCTO	FY21 IT Assessments	$126,644
HSEMA	DGS	EOC Enhancement	$357,740
HSEMA	Office of Finance Resource Management	Agency Purchase Cards	$60,000
HSEMA	DCHR	Employee Screening Services	$2,999
HSEMA	OCTO	Webelos Integration	$50,884
HSEMA	DOEE	District Mitigation Plan	$22,622

8. **For FY20 and FY21, to date, please identify any special purpose revenue funds maintained by, used by, or available for use by the agency. For each fund identified, provide:**

   a. **The revenue source name and code;**
   b. **The source of funding;**
   c. **A description of the program that generates the funds;**
   d. **The amount of funds generated by each source or program;**
   e. **Expenditures of funds, including the purpose of each expenditure;**

f. Whether expenditures from the fund are regulated by statute or policy, and if so, how; and

g. The current fund balance.

HSEMA does not maintain, use, or have available for use, any special purpose revenue funds.

9. For FY20 and FY21, to date, please list all purchase card spending by the agency, the employee making each expenditure, and the general purpose of each expenditure.

Please see attachment "Q9 HSEMA".

10. Please list all capital projects in the financial plan for the agency or under the agency's purview in FY20 and FY21, to date, and provide an update on each project, including the amount budgeted, actual dollars spent, and any remaining balances (please also include projects for the benefit of the agency that are in the budget of the Department of General Services or another agency). In addition, please provide:

a. A narrative description of all capital projects begun, in progress, or concluded in FY19, FY20, and FY21, to date, including the amount budgeted, actual dollars spent, any remaining balances, and the work undertaken;

b. An update on all capital projects planned for the four-year financial plan;

c. A description of whether the capital projects begun, in progress, or concluded in FY19, FY20, and FY21, to date, had an impact on the operating budget of the agency. If so, please provide an accounting of such impact; and

d. A description and the fund balance for any existing allotments.

HSEMA received and was allotted $4.25M in FY20 capital funding to accomplish one project: the renovation of the District's Emergency Operations Center. To date, HSEMA has worked with the architectural/engineering (A/E) vendor to complete the programming/design phase. HSEMA is now in the schematic design and permit/construction document phases and will work with the Department of General Services to initiate the construction solicitation by September 2021. HSEMA invested $590,841 in federal grant dollars to supplement the $4.25M in capital funding. To date, HSEMA has spent $163,101 and obligated $427,740 in federal grant dollars. This includes costs related to the A/E service contract and the technology integration contract. The anticipated completion date is 18 months.

11. Please provide a list of all budget enhancement requests (including capital improvement needs) for FY20 and FY21, to date. For each, include a description of the need and the amount of funding requested.

HSEMA works with the Office of the City Administrator to develop its budget. The FY2020 and FY2021 budgets submitted by the Mayor to the Council reflect those efforts.

12. Please list, in chronological order, each reprogramming in FY20 and FY21, to date, that impacted the agency, including those that moved funds into the agency, out of the agency, or within the agency. Include known, anticipated reprogrammings, as well as the revised, final budget for your agency after the reprogrammings. For each reprogramming, list the date, amount, rationale, and reprogramming number.

Please see attachment "Q12 HSEMA".

13. Please list each grant or sub-grant *received by* your agency in FY20 and FY21, to date. List the date, amount, source, purpose of the grant or sub-grant received, and amount expended.

Grant Program	Date	Amount	Expended to date	Source	Purpose
Emergency Management Performance Grant (EMPG)	4/25/2020	$3,115,544	$2,945,551	DHS-FEMA	The purpose of the FY 2020 EMPG Program is to give grants to assist state, local, tribal, and territorial governments in preparing for all hazards, as authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).
Emergency Management Performance Grant (EMPG) – COVID-19 Supplemental	5/15/2020	$877,618	$877,618	DHS-FEMA	The purpose of the FY 2020 EMPG COVID-19 Supplemental grant is to provide supplemental funding to support state emergency management response to the COVID-19 pandemic
Homeland Security Grant Program (HSGP) - includes the State Homeland Security Program (SHSP) and Urban Areas Security Initiative (UASI)	9/08/2020	Total: $57,279,000 UASI: $51,750,000 SHSP: $5,529,000	Total: $3,575,466 UASI: $2,434,477 SHSP: $1,140,989	DHS-FEMA	The FY 2020 HSGP provides funding for planning, organization, equipment, training, and exercise needs of states and high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. It is composed of the UASI and SHSP.
Nonprofit Security Grant Program (NSGP)	8/29/2020	$4,084,014	$0	DHS-FEMA	NSGP provides funding support for target hardening activities to nonprofit organizations that are at high risk of a terrorist attack and located within one of the UASI-eligible urban areas. DC

					had 48 successful applicants in FY2020.
Targeted Violence and Terrorism Prevention	9/23/2020	$150,000	$0	DHS	TVTP supports the DHS strategic framework for countering terrorism and targeted violence by establishing and enhancing locally based prevention programs. This award focuses on enhancing the ability of state partners to identify and respond to individuals at risk of mobilizing to violence.
Securing the Cities Program	9/11/2020	$1,999,141	$0	DHS	The Securing the Cities program (STC) is a DHS initiative to expand state/local radiation detection capability in major urban areas. This award is intended to sustain the current National Capital Region STC program established through prior grant awards.
Crisis Counseling – Immediate Services Program (COVID-19)	5/27/2020	$350,507	$208,527	DHS-FEMA	The CCP-ISP program is part of FEMA's support to the COVID-19 response and provides crisis counseling support to individuals and families affected by the incident. The program a collaboration between FEMA and HHS/SAMHSA. The sole recipient of funds is the Department of Behavioral Health.
Presidentially Declared Disaster – Public Assistance Grant (COVID – 4502)	4/17/2020	$147,479,666	$147,479,666	DHS-FEMA	The Presidentially Declared Disaster – Public Assistance Grant is authorized under the Stafford Act and provides reimbursement to States and localities for costs incurred by governments to respond to and recover from major disasters – this award is for Emergency Protective Measures relating to COVID-19. The amount is the current obligated amount for approved projects, and changes as projects are approved.
Presidentially Declared Disaster – Public Assistance Grant	1/11/2021	$0	$0	DHS-FEMA	The Presidentially Declared Disaster – Public Assistance Grant is authorized under the Stafford Act and provides

(Inauguration – 3553)					reimbursement to States and localities for costs incurred by governments to respond to and recover from major disasters – this award is for Emergency Protective Measures relating to the Presidential Inaugural period (1.12 – 1.24). The amount is the current obligated amount for approved projects, and changes as projects are approved.
Hazard Mitigation Assistance Grants (HMA) – includes Pre-Disaster Mitigation Grant Program (PDM), Flood Mitigation Assistance (FMA), Hazard Mitigation Grant Program (HMGP)	9/24/2020	$215,000	$0	DHS-FEMA	The flood mitigation assistance grant program funds provide funds for planning and projects to reduce or eliminate risk of flood damage that are insured annually under the National Flood Insurance Program. The award will support hazard mitigation and resiliency planning for the Southwest Waterfront neighborhood and DC Water Blue Plains Advanced Wastewater Treatment Plant.

a. How many FTEs are dependent on grant funding?

All of HSEMA's FTEs are either fully or partially dependent on grant funding (total of 142 FTEs).

b. What are the terms of this funding?

Grant-funded employees work in support of the federal grant programs' goals, which are emergency preparedness and response, building homeland security capabilities, and reducing or eliminating long-term risk to people and property from natural hazards.

c. If it is set to expire, what plans, if any, are in place to continue funding the FTEs?

The current grant programs are multi-year and will not expire this fiscal year. Continued funding is dependent on Congress appropriating FY2021 grants. HSEMA is currently working with DC Office of Federal and Regional Affairs (OFRA) as well as our partners in the federal agencies, FEMA and USDHS, to ensure that the District continues to receive the homeland security grant funding necessary to further our mission.

14. Please list each grant or sub-grant ***granted by* your agency in FY20 and FY21, to date. List the date, amount, source, and purpose of the grant or sub-grant granted.**

Please see attachment "Q14 HSEMA".

15. Please list each contract, procurement, and lease entered into or extended and option years exercised by your agency during FY20 and FY21, to date. For each contract, procurement, or lease, please provide the following information, where applicable:

a. The name of the party;
b. The nature of the contract, procurement, or lease, including the end product or service;
c. The dollar amount of the contract, procurement, or lease, including amount budgeted and amount actually spent;
d. The term of the contract, procurement, or lease;
e. Whether it was competitively bid;
f. The name of the agency's contract monitor(s) and the results of any monitoring activity; and
g. The funding source.

Please see attachment "Q15 HSEMA".

16. Please list and describe all pending and closed lawsuits that name or named the agency as a party in FY20 and FY21, to date, and include an explanation about the issues involved in each case. Identify which cases on the list are lawsuits that potentially expose the District to significant financial liability or could result in a change to agency practices and describe the current status of the litigation.

There is no pending nor closed lawsuits in FY20 or FY21, to date that name the agency as a party.

17. Please list all judgments against and settlements executed by the agency or by the District on behalf of the agency, of any amount, in FY20 or FY21, to date, and provide the parties' names, the date on which the judgment was issued or settlement was executed, the amount of the judgment or settlement, and if related to litigation, the case name, docket number, and a brief description of the case. Include non-monetary costs such as backpay and leave restoration. If unrelated to litigation, please describe the underlying issue or reason for the judgment or settlement (e.g. excessive use of force, wrongful termination, sexual harassment). Please also describe any matters which are currently in settlement negotiations or for which a judgment is imminent.

There are no judgments against, or settlements executed by the agency or by the District on behalf of the agency in FY20 or FY21, to date.

18. Did the agency use outside counsel in FY20 and FY21, to date? If so, for what matter(s) and in what amount(s)?

Gregory Evans, when serving as General Counsel for the Office of Unified Command, provided general legal services to HSEMA in FY20, during the time when HSEMA's General Counsel position was vacant. (March 2019-December 2019).

19. Please list the administrative complaints or grievances that the agency received in FY20 and FY21, to date, broken down by source. Please describe the process utilized to respond to any complaints and grievances received and any changes to agency policies or procedures that have resulted from complaints or grievances received. For any complaints or grievances that were resolved in FY20 or FY21, to date, describe the resolution.

The agency received six administrative complaints and three grievances in FY20 and FY 21, to date. Administrative complaints are handled according to the nature of the complaint. Complaints regarding employee conduct are handled by HSEMA management and human resources in accordance with District Personnel Instruction No. 16-18. Complaints regarding sexual harassment or misconduct are handled in accordance with Mayor's Order 2017-313: Sexual Harassment Policy, Guidance and Procedures. Complaints regarding discrimination are handled in accordance with the Office of Human Rights (OHR) complaint process. The agency follows the grievance policies and procedures established in §§ 1626 through 1635 in the District Personnel Manual (DPM) for non-union employees. Union employees have the option to follow the grievance/arbitration procedures established in Article 24 of the Collective Bargaining Agreement (CBA) or the grievance policies and procedures established in §§ 1626 through 1635 in the DPM. The current CBA between HSEMA and the National Association of Government Employees Local R3-08, originally effective October 1, 2014 through September 20, 2017, has expired. The agreement remains in force until either party to the agreement states the desire to renegotiate. For reference, please see CBA article 34 section D the current CBA, attached as attachment "Q33 HSEMA".

The following are the nine matters addressed during FY20:

- Two matters involved complaints/allegations of discrimination, which were handled and resolved via the District's Equal Employment Opportunity (EEO) review process.
- One complaint of sexual harassment, which was investigated and dismissed for lack of evidence.
- One complaint of sexual harassment, which is currently under investigation by OHR.
- One complaint of denial of reasonable accommodations, which is currently under review by OHR.
- One complaint of unprofessional language in the workplace. The matter was investigated internally and resolved via a corrective discipline action.
- One matter of an employee challenging a low-level discipline action. The matter was resolved in the employee's favor via the DPM's grievance process.

- Two grievances filed by the NAGE labor union. The first challenged the termination of a collective bargaining member during the probationary period. This was denied by the agency because NAGE lacks ability to grieve probationary terminations. The second matter involved a grievance requesting administrative pay for bargaining unit members during the COVID telework posture. NAGE invoked arbitration but withdrew the grievance before the hearing commenced.

- The agency has not received an administrative complaint during FY21.

20. Please describe the agency's procedures for investigating allegations of sexual harassment, sexual misconduct, or discrimination committed by or against agency employees. List and describe any allegations relating to the agency or its employees in FY20 and FY21, to date, and whether and how those allegations were resolved (e.g. a specific disciplinary action, such as re-training, employee transfer, suspension, or termination).

a. Please also identify whether the agency became aware of any similar matters in FY20 or FY21, to date, through means other than an allegation, and if so, how the matter was resolved (e.g. sexual harassment was reported to the agency, but not by the victim).

HSEMA follows the procedures for investigating allegations of sexual harassment and sexual misconduct in accordance with Mayor's Order 2017-313 Sexual Harassment Policy, Guidance and Procedures. HSEMA has two Sexual Harassment Officers who received the required training from DCHR. In FY20 and FY21, to date, the agency received two complaints of sexual harassment. One complaint was unsubstantiated as it did not rise to a violation as defined in Mayor's Order 2017-313. The other complaint is pending resolution. Also, the agency has not become aware of a sexual harassment or misconduct matter through a means other than an allegation.

HSEMA follows the OHR process for investigating allegations of discrimination committed by or against agency employees. Individuals must first participate in EEO counseling to attempt informal resolution. If informal resolution is not achieved, the individual may file a formal complaint through OHR.

21. Please provide the Committee with a list of the total workers' compensation payments paid by the agency or on the agency's behalf in FY20 and FY21, to date, including the number of employees who received workers' compensation payments, in what amounts, and for what reasons.

HSEMA did not process any workers' compensation payments during FY20 or FY21, to date.

22. Please list and describe any ongoing investigations, audits, or reports on the agency or any employee of the agency, or any investigations, studies, audits, or reports on the agency or any employee of the agency that were completed during FY20 and FY21, to date.

In FY2020 FEMA conducted a monitoring visit to review HSEMA management of FEMA grants for proper compliance, oversight, and financial management. The monitoring visit originally scheduled for spring 2020 was postponed due to COVID until September 2020 (virtually). The final report issued in November 2020 had no findings and required no specific corrective actions.

The federal Government Accountability Office (GAO) pursued an Audit of National Independence Day Celebration in FY 2020. The federal Government Accountability Office (GAO) pursued an Audit of National Independence Day Celebration in FY 2020. On March 9th, an exit interview was conducted, and GAO will issue a final report in the upcoming months.

The DC Office of the Inspector General (OIG) is performing an ongoing Audit of the District's Procurements during the COVID-19 Public Health Emergency that started in FY2020.

23. Please describe any spending pressures the agency experienced in FY20 and any anticipated spending pressures for the remainder of FY21. Include a description of the pressure and the estimated amount. If the spending pressure was in FY20, describe how it was resolved, and if the spending pressure is in FY21, describe any proposed solutions.

The agency did not experience any spending pressures in FY20 and does not anticipate any spending pressures in FY21.

24. Please provide a copy of the agency's FY20 performance plan. Please explain which performance plan objectives were completed in FY20 and whether they were completed on time and within budget. If they were not, please provide an explanation.

Please see attachment "Q24 HSEMA" for the FY20 performance plan.

HSEMA fully met all but four of its key performance indicator (KPI) targets in FY20 on time and within budget. Four KPIs fell short of target levels.

- The first of these measures, "Percent of distributable analytic products co-authored with one or more federal, state or local partners" did not meet its target of 10% with only 5.1% of distributable products being co-authored. As an all-hazards fusion center, many of the NTIC's resources were leveraged towards the COVID-19 response throughout FY20. COVID-related production does not lend itself to coauthoring with traditional fusion center partners, as it is specific to the NTIC's Area of Responsibility AOR.

- The agency also fell short of its 10% target for "Percent increase in the number of subscribers to fusion center situational and analytic product distribution lists" with a 69% decrease in subscribers. During FY20 Q4, the NTIC scrubbed its distribution list and required all recipients remaining on the list to sign a new non-disclosure agreement (NDA) to continue receiving products. This resulted in the removal of approximately 3,000 legacy recipients, mostly from inactive email addresses.
- The agency did not meet its target of 95% for "Percent of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements." Though the majority of staff have completed their training, changes to the staff members aligned to this funding source and limited bandwidth for training during COVID response were limiting factors in meeting this target.
- Finally, the agency nearly met its target for "Percent of federal subgrants issued within 45 days of award receipt" achieving 88.5% of the 90% target. Response to the COVID-19 pandemic caused shifts in the decision-making timeline that delayed the agency's ability to issue subawards to regional recipients, resulting in an actual distribution number slightly below the target level but well above the federally required level of 80%.

HSEMA also had three incomplete initiatives in FY20 – primarily the result of diverting resources from planned initiatives to support the District's COVID response.

- The District's IMT Academy did not graduate its first cohort because our ability to deliver classes and conduct exercises is on hold indefinitely through the end of the agency's COVID-19 response operations. We have reset our completion target for the first cohort to the end of 2021.
- The agency did not fully stand up physical risk assessment teams due to staff turnover and postponed trainings in light of COVID-19. Additionally, in the last quarter of the fiscal year, NTIC resources were devoted primarily to preparing for the 59th Presidential Inauguration resulting in additional delays.
- Finally, the agency did not complete the design process for an upgraded Emergency Operations Center because the initial design was amended to accommodate adjusted requirements, and funding intended to support these changes was unavailable due to COVID.

25. Please provide a copy of your agency's FY21 performance plan as submitted to the Office of the City Administrator.

Please see attachment "Q25 HSEMA" for the FY21 performance plan.

26. Please describe any regulations promulgated by the agency in FY20 or FY21, to date, and the status of each.

Pursuant to the "District of Columbia Government Continuity of Operations Plans Amendment Act of 2019," HSEMA began requesting that agencies designate a backup Continuity of Operations Plan (COOP) Coordinator in FY20. This will now be required of agencies as a result of the new COOP legislation. Currently, 34 of 42 cabinet-level agencies have designated a backup COOP Coordinator.

In addition, independent agencies were not required to complete a COOP plan under Mayor's Order 2012-61. The new COOP legislation extends the requirement to these agencies, and thus these agency profiles have been set up in Coordination, Operations, Readiness, Engagement (CORE) DC and prepopulated by HSEMA with the addresses of the District's real estate portfolio and a database of each agency's functions to reduce the workload of individual agencies to complete COOP requirements.

The legislation also requires the development of an annual COOP progress memo that include the Designation of a District COOP Program Manager. The 2020 annual COOP progress memo has been transmitted to the City Administrator and Councilmember Allen.

27. Please provide the number of FOIA requests for FY20 and FY21, to date, that were submitted to your agency. Include the number granted, partially granted, denied, and pending. In addition, please provide the average response time, the estimated number of FTEs required to process requests, the estimated number of hours spent responding to these requests, and the cost of compliance.

FOIA	FY20	FY21, to date (02/23/21)
Number of requests submitted to HSEMA	103	43
Number of requests granted	31	5
Number of requests partially granted	2	1
Number of requests of denied	1	0
Number of requests pending	7	24
Not Agency Record	64	30
Average response time	8.1	11.94
Estimated Number of FTEs	1	1
Estimated Number of hours	520	88
Cost of compliance	$26,847	$4,543

28. Please provide a list of all studies, research papers, reports, and analyses that the agency prepared or for which the agency contracted during FY20 and FY21, to date. Please state the status and purpose of each. Please submit a hard copy to the Committee if the study, research paper, report, or analysis is complete.

In FY20 HSEMA's Resilience Bureau initiated two supply chain analysis projects, funded by the U.S. Department of Homeland Security and conducted for HSEMA by Idaho

National Laboratory, that will be ongoing through FY22. The Bureau also initiated a project funded by FEMA and being conducted with contractor support to develop an emergency food and water plan for the NCR for catastrophic events; that project will be ongoing through FY22.

A draft report was developed under the Disability Integration Initiative (DII) Emergency Shelter Capital Project Report and the Emergency Shelter Database, Post-Emergency Canvassing Operations Plan and Transportation Gap Analysis for Emergency Evacuation. It is pending final review.

Due to the sensitive nature of HSEMA's non-public documents, only *unclassified* Intelligence Bulletins are available for Council review. In addition, please see attachment "Q28 HSEMA" for copies of distributed cyber threat bulletins in FY20 and FY21, to date.

29. Please list in descending order the top 25 overtime earners in your agency in FY20 and FY21, to date, if applicable. For each, state the employee's name, position number, position title, program, activity, salary, fringe, and the aggregate amount of overtime pay earned. Please describe the process the agency uses to determine which employees are granted overtime.

Please see attachment "Q29 HSEMA." Due to the demands of the District's COVID-19 response and HSEMA's lead role in coordination, many HSEMA employees worked shifts much longer than their regular tours of duty. This volume of overtime was specific to the early months of the COVID-19 response.

HSEMA follows the District Personnel Manual Chapter 11 and 12 and the Collective Bargaining Agreement (CBA) when administering overtime for our employees. Also, overtime is managed at the agency bureau level. Bureau managers approve employees for overtime if there is an operational need. Please see the current CBA, attachment "Q33 HSEMA."

30. For FY20 and FY21, to date, please provide a list of employee bonuses or special pay granted that identifies the employee receiving the bonus or special pay, the amount received, and the reason for the bonus or special pay.

Fiscal Year	Employee Name	Position Title	Bonus Pay	Special Award	Reason
20	Steven Benefield	Communications Management Specialist	$25,000	N/A	Retirement

31. For FY20 and FY21, to date, please list each employee separated from the agency with separation pay. State the amount and number of weeks of pay. Also, for each, state the reason for the separation.

HSEMA did not have any employees separate from the agency with separation pay in FY20 or FY21, to date.

32. Please provide the name of each employee who was or is on administrative leave in FY20 and FY21, to date. In addition, for each employee identified, please provide: (1) their position; (2) a brief description of the reason they were placed on leave; (3) the dates they were/are on administrative leave; (4) whether the leave was/is paid or unpaid; and (5) their current status.

Name	Title	Reason	Time Frame	Paid/ Unpaid	Current Status
Frederick Goldsmith	Deputy Chief of Operations	Operations pending final decision on corrective or adverse action per DPM § 1619.1.	10/10/19-2/2/20	Paid	Returned to work.

33. Please provide each collective bargaining agreement that is currently in effect for agency employees. Include the bargaining unit and the duration of each agreement. Note if the agency is currently in bargaining and its anticipated completion.

The current Collective Bargaining Agreement (CBA), originally effective October 1, 2014 through September 20, 2017, and remains in effect until one party requests negotiation. Please see the current CBA, attached as "Q33 HSEMA."

34. If there are any boards, commissions, or task forces associated with your agency, please provide a chart listing the names, number of years served, agency affiliation, and attendance of each member. Include any vacancies. Please also attach agendas and minutes of each board, commission, or task force meeting in FY20 or FY21, to date, if minutes were prepared. Please inform the Committee if the board, commission, or task force did not convene during any month.

The Homeland Security Commission currently has two vacancies. The most recent meeting was held on March 5, 2021. Additional information for the Homeland Security Commission is included in the table below:

Commissioner	Confirmation Date/Term Beginning	Term End	Residence	Attendance
Brad Belzak (Chair)	December 8, 2017	February 22, 2022 (Reappointment approved by DC Council in January 2020)	Ward 2	February 26, 2020; June 10, 2020; July 10, 2020; July 31, 2020; August 6, 2020; August 13, 2020; August 20, 2020; September 11, 2020
Philip McNamara	July 11, 2017	February 22, 2022 (Reappointment approved by DC Council in January 2020)	Ward 1	February 26, 2020; June 10, 2020; July 10, 2020; July 31, 2020; August 6, 2020; August 20, 2020; September 11, 2020
Edward Pearson	December 18, 2018	February 22, 2022	Ward 7	February 26, 2020; June 10, 2020; July 10, 2020; July 31, 2020; August 13, 2020; August 20, 2020;
Joanna Turner	December 18, 2018	February 22, 2022	Ward 6	February 26, 2020; July 10, 2020; July 31, 2020; August 13, 2020;
Brian Baker	December 18, 2018	February 22, 2022	Ward 6	February 26, 2020; June 10, 2020; July 10, 2020; July 31, 2020; August 6, 2020; August 13, 2020; September 11, 2020

Please see attachments "Q34 Part 1 HSEMA" for the FY20 and FY21 agendas and "Q34 Part 2 HSEMA" for the open meeting minutes.

35. Please list all reports or reporting currently required of the agency in the District of Columbia Code or Municipal Regulations. Provide a description of whether the agency is in compliance with these requirements, and if not, why not (e.g. the purpose behind the requirement is moot, etc.).

The "Homeland Security, Risk Reduction, and Preparedness Amendment Act of 2006" requires the Executive to submit to the Council of the District of Columbia an annual report describing the current level of preparedness in the District. Work on the next annual report is underway.

36. Please provide a list of any additional training or continuing education opportunities made available to agency employees. For each additional training or continuing education program, please provide the subject of the training, the names of the trainers, and the number of agency employees that were trained.

Course Name/Subject	Number of Participants (HSEMA Staff, District and National Capital Region)	Training Entity Providing Instruction
Language Access Training	52	HSEMA
ICS - 300, Intermediate ICS for Expanding Events	18	HSEMA
L-967: NIMS ICS All-Hazards Logistics Section Chief	10	Wiland Associates
L-950: NIMS ICS All-Hazards Incident Commander	12	Wiland Associates
L-964: NIMS ICS All-Hazards Situation Unit Leader	36	Wiland Associates
MGT-323 Instructor Development Workshop	15	LSU-NCBRT
L-965: NIMS ICS All-Hazards Resource Unit Leader	21	Wiland Associates
ERisk Incident Reporting Portal Training	10	DCHR
Leadership Management Series: Leading with Strategy	20	Andres Marquez-Lara
Individual Assistance/Public Assistance Workshop	19	FEMA
2020 DC Emergency Operations Center Series 1 - Overview	16	HSEMA
Emergency Liaison Officer Training (ELO)	24	HSEMA
EOC Planning Coordination Section Orientation	20	HSEMA
2020 DC Emergency Operations Center Series 1 - Overview	36	HSEMA
Emergency Liaison Officer Training (ELO)	20	HSEMA
FEMA Environmental Historic Preservation	11	FEMA
FEMA EHP Roadshow Training	11	FEMA
G300 - Intermediate ICS for Expanding Events	24	HSEMA
Basic PIO combined with JIS/JIC	36	Contractor
EOC Virtualization- Big 8 Connectivity	64	HSEMA

EOC Virtualization- Election Day Session	70	HSEMA
EOC Virtualization- Seminar Session	13	HSEMA
EOC Virtualization- Seminar Session	34	HSEMA
EOC Virtualization	18	HSEMA
EOC Virtualization	16	HSEMA
G0290: Basic Public Information Officers	13	Contractor
G0291: Joint Information System/Center Planning for Tribal, State, and Local Public Information Officers	12	Contractor
HA05003 - CORE DC Signature Request	82	HSEMA LMS
HA05004 - CORE DC Notebook	89	HSEMA LMS
HA05005: CORE DC Agency Profiles	40	HSEMA LMS
HA05006: CORE DC Continuity of Operations	30	HSEMA LMS
HA05007: CORE DC Performance Management-Employee	97	HSEMA LMS
HA05008: CORE DC Performance Management-Manager	21	HSEMA LMS
HA05009: CORE DC Purchase Request	22	HSEMA LMS
HA05010: CORE DC 101	3	HSEMA LMS
XA06003 - Mass Care Task Force (MCTF) Training I (D.C. DHS): MCTF Training I: 1st Class	37	DC Human Servs
XA06003 - Mass Care Task Force (MCTF) Training I (D.C. DHS): MCTF Training I: 2nd Class	32	DC Human Servs
Grocery Point of Distribution (POD) Training	63	DC Human Servs/HSEMA LMS
Language Access Training	76	HSEMA
G0300 - ICS 300	16	HSEMA
HA05011- EOC 101-Basic Emergency Operations Center (EOC)	15	HSEMA
IS0230.d: Fundamentals of Emergency Management	9	FEMA/HSEMA LMS
HA05004 - CORE DC Notebook	7	HSEMA LMS

HA05003 - CORE DC Signature Request	6	HSEMA LMS
IS0235.C: Emergency Planning	6	FEMA/HSEMA LMS
HA05010 - CORE DC 101	5	HSEMA LMS
IS-200: Basic Incident Command System for Initial Response	5	FEMA/HSEMA LMS
IS-0100: Introduction to the Incident Command System	4	FEMA/HSEMA LMS
IS0242.B: Effective Communication	4	FEMA/HSEMA LMS
HA05005 - CORE DC Agency Profiles	3	HSEMA LMS
IS0244.B: Developing and Managing Volunteers	3	FEMA/HSEMA LMS
IS2200: Basic Emergency Operations Center Functions	3	FEMA/HSEMA LMS
HA05006 - CORE DC Continuity of Operations	2	HSEMA LMS
IS0120.C: An Introduction to Exercises	2	FEMA/HSEMA LMS
HA05002 - HSEMA Language Access Training	1	HSEMA LMS
HA05012: EOC 102- Emergency Liaison Officer (ELO) Roles and Responsibilities	1	HSEMA LMS
IS0240.B: Leadership and Influence	1	FEMA/HSEMA LMS
IS0241.B: Decision Making and Problem Solving	1	FEMA/HSEMA LMS
IS0393.B - Introduction to Hazard Mitigation	1	FEMA/HSEMA LMS

37. Please describe any initiatives that the agency implemented in FY20 or FY21, to date, to improve the internal operations of the agency or the interaction of the agency with outside parties. Please describe the results, or expected results, of each initiative.

See attachment "Q24 HSEMA" for our FY20 Performance Accountability Report (PAR). Additionally, please see FY21's first quarter reporting information, detailing our initiatives and progress in achieving the results for the current fiscal year, below:

Initiative: In FY21, HSEMA will partner with additional agencies to successfully apply for increased mitigation funding from FEMA's new Building Resilient Infrastructure and Communities program.

First Quarter Update: HSEMA has partnered with additional agencies to apply for increased mitigation funding from FEMA's Hazard Mitigation Assistance grants. To date, we have applied for over $40 million dollars in grant funds to support agencies and stakeholders, including Department of General Services, Department of Energy and Environment, Office of the Deputy Mayor for Planning and Economic Development and more. The announcement selection of awardees will be determined in the 3rd quarter.

Initiative: HSEMA will increase the preparedness of residents in neighborhoods at disproportionately higher risk of impact from natural and man-made hazards Specifically, HSEMA will conduct at least 10 community outreach events in wards 7 and 8 to advise residents of the specific risks to their communities and provide access to preparedness resources. Events may be conducted virtually or in person as needed to support COVID mitigation measures.

First Quarter Update: To date, the Mitigation Program conducted at least 4 outreach events in ward 7 and 8 to advise residents of the specific risks to their communities and provide access to preparedness resources.

Initiative: HSEMA will coordinate the District's agency-wide consequence management planning and execution for the 2021 Presidential Inauguration with District, regional, and federal partners, and develop the District's comprehensive after-action report. This will include coordination for both official Inauguration events as well as associated events including planned and unplanned demonstrations and other first amendment activity.

First & Second Quarter Update: On January 6, 2021, a mob of President Trump supporters stormed the US Capitol Building to protest the certification of election results just two weeks before the Inauguration. Beyond the massive response to the siege from the District government - with coordination and support from HSEMA, this event required a wholesale reevaluation of the planning for the Inauguration which was already upended by COVID-19 and the delay in certification of the election. HSEMA expanded EOC support and executed key coordination activities with regional and federal partners to enhance the event security posture. HSEMA enhanced the emergency operations center (EOC) posture for an additional 8 days.

Initiative: In FY21, HSEMA will continue to upgrade the capabilities of the District's Emergency Operations Center (EOC). Working with the Department of General Services, HSEMA will complete the next phase of redesign of the EOC floor space to increase efficiency and maximize capacity during operations. HSEMA expects to complete the design phase and initiate the construction solicitation process by the end of FY21.

First Quarter Update: In Q1, HSEMA completed the programming phase of the overall design. This portion of the design phase is approximately 40% of the overall design effort. HSEMA is confident it will complete the design phase and initiate the construction solicitation by September 30, 2021.

38. What are the agency's top five priorities? Please explain how the agency expects to address these priorities in the remainder of FY21. How did the agency address its top priorities listed for this question last year?

In FY21, HSEMA will continue to address the top five priorities introduced in FY19, building upon our progress over the past year:

- *Strengthening HSEMA's organizational performance* – HSEMA will improve organizational performance by building on process improvements made last year, continuing to integrate our intelligence and emergency management functions, and by developing and deploying a key piece of technology (WebEOC) that will improve situational awareness of the District. In FY20, we continued to refine current policies, as well as updated administrative tools and processes (e.g., developed the purchase request forms and travel forms in WebEOC), and continuing the quarterly performance reporting process and re-training all staff.
- *Optimizing the way HSEMA spends grant dollars* – HSEMA will optimize the way it spends grant money by evaluating return on investment for key grant programs. In FY20, the Agency continued examining current spending against historical spending, preparing for federal budget cuts potentially impacting our grant programs, and continuing to refine the annual budgeting cycle to better track spending.
- *Building a regional intelligence capability* – HSEMA continues to seek expansion of the capabilities of the National Capital Region Threat Intelligence Consortium (NTIC). HSEMA will continue to invest resources for hiring and training new analysts and improve the quality of our analytic products, and ensure proactive information sharing with other fusion center and intelligence community partners.
- *Develop a whole of community approach to disaster management and disaster preparedness* – HSEMA will continue to focus on improving outreach to two key constituencies in the District – the private industry and faith-based communities. Moving the needle forward with our identified audience, in FY20, we continued to engage the District's faith-based community and private sector community leading up to planned events and following spontaneous events that occurred from June – December.
- *Become a more anticipatory organization* – HSEMA is proactively acquiring and utilizing new technology to improve our operational and preparedness capabilities. HSEMA has created and continues to develop a suite of weather-related products to help the District better prepare for the impacts of severe weather events. Additionally, the agency continues to invest resources in impending threat analyses ahead of multiple first-amendment events.

39. Please list each new program implemented by the agency during FY20 and FY21, to date. For each initiative, please provide:

a. A description of the initiative;
b. The funding required to implement the initiative; and

c. Any documented results of the initiative.

Improved Operational Response Capacity
Description: HSEMA has expanded the size of its staff that is dedicated to incident management and response to ensure that it always has adequate staff available to manage incidents when they arise. In 2020-21, within the Operations Division, HSEMA increased the size of its Response Readiness Bureau from three to eight staff members for initial incident response.

Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: This complements the on-duty staff available 24 hours per day within the JAHOC. HSEMA also expanded the cadre of staff from outside of the Operations Division responding on a voluntary basis to augment incident staffing. Finally, HSEMA expanded the Mobile Situational Awareness Teams (MSAT) that mobilize during special events and incidents to assess damage and impacts to District government operations. This is part of a three-year focus on enhancing the agency's incident management capacity, especially to manage multiple concurrent incidents within the District.

Interfaith Preparedness & Advisory Group (IPAG)
Description: The IPAG mission is to provide a platform for Faith-Based Organizations (FBO) to exchange information among themselves and with District Agency representatives concerning threats, vulnerabilities, best security practices, and protective measures related to the safety and security of their congregations and facilities. The IPAG is sponsored by the Mayor's Office of Religious Affairs (MORA), HSEMA, and the Metropolitan Police Department (MPD). The IPAG provides a platform for faith-based organizations to exchange information with security and preparedness professionals on threats, vulnerabilities, best security practices, and protective measures related to the safety and security of congregations and facilities.

Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results (Quarterly Meetings): On December 12, 2019 IPAG hosted its final quarterly meeting of 2019 at Shepard's Baptist Church and took time to reinforce how to report suspicious activity, as well as listening to presentations from FBI's Private Partnership Engagement team and DC's Department of Behavioral Health Community Response Team. IPAG members also received TECC kits if they attended the "Until Help Arrives" training.

*Updated Training for Emergency Liaison Officers (ELO***)**
Description: During emergencies and planned major events, District agencies and outside partners send staff to the District's Emergency Operations Center (EOC) to coordinate operations and foster collaboration. This role is known as the Emergency

Liaison Officer (ELO). This initiative is designed to improve the training course that HSEMA provides to all ELOs by taking feedback from ELOs and incorporating lessons learned during the very previous two years to provide better and more effective training for ELOs.

Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: HSEMA has provided EOC 101- Basic Emergency Operations Center training to 42 ELOs in FY21.

Joint All-Hazards Operations Center (JAHOC) Enhancements
Description: HSEMA is working to enhance the District's JAHOC operations by increasing hands-on training opportunities; developing additional watch and warning capabilities; expanding representation of other District agencies; and integrating the fusion center's intelligence capabilities into daily watch and warning operations.

Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: HSEMA has expanded our supervisor staffing in the JAHOC to provide one-on-one training opportunities for staff. The agency has also added three staff members to each shift to enhance existing capabilities and expand our services. HSEMA implemented an updated training program for JAHOC watch. The agency has also integrated an intelligence analyst into the JAHOC. In addition, HSEMA fully integrated a 24/7 intelligence component into the JAHOC and integrated our local and FEMA regional watch component.

Incident Coordination and Support Teams
Description**:** Building upon the success of the team that manages the District's Emergency Operations Center, HSEMA is working with a number of District agencies and outside partners, chiefly FEMS, to build deployable incident management teams. HSEMA is also updating the agency fleet to support collaboration at incidents and events.

Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: HSEMA has increased the frequency with which we are deploying incident coordination and support staff to incidents, specifically residential fires with displacements. HSEMA also dedicated additional resources to developing a replicable safety program for our deployable staff to share with our partners for them to implement within their own agencies in 2020.

Disability Integration Initiative (DII)
Description: The District of Columbia and Disability Advocacy groups reached a

groundbreaking settlement agreement May 03, 2019. Under the historic settlement, the District has agreed to a comprehensive three-year implementation plan that includes: (1) creating a Disability Community Advisory Group that will provide disability-specific recommendations for emergency plans and trainings, (2) ensuring that emergency-related public communications are disseminated in accessible formats, (3) considering physical accessibility as a priority when opening emergency shelters, (4) creating a Post-Emergency Canvassing Operation plan, (5) ensuring that transportation resources are sufficient to meet the potential demand for accessible transportation during emergencies, and (6) creating and implementing a work plan to improve procedures for evacuating people with disabilities from high-rise buildings. Through the completion of these requirements updates to the District's emergency plans to provide individuals with disabilities equal access to critical government services.

Funding: FY2020 DII was funded under the Urban Area Security Initiative and for FY2021, DII submitted a proposal for funding under the Homeland Security Grant Program.

Results: DII has convened multifunctional working groups comprised of District agencies and community advocates to assist in updating and integrating emergency plans with inclusive strategies. A Mayor's Order and Memorandum of Agreement support the participation in completing the initiative holistically for the District. All milestones to date have been completed including, but not limited to, updating the HSEMA mobile app and website; Siteimprove, a web-based tool provided from OCTO to track 508 compliance[1] for all DC agency web pages; emergency sheltering analysis; and quarterly reports capturing progress in all the working groups. Below are the milestones for FY20 & FY21:

- Jan 2020 – Produced the Shelter Gap Analysis Report.
- Jan 2020 – Held meeting with the DII Working Groups.
- Feb 2020 – Held meeting with the DII Working Groups.
- Mar 2020 – Held quarterly meeting with the Disability Community Advisory Group (DCAG). The DCAG consists of eleven, non-government organizations that serve the disability community.
- Mar 2020 – Nov 2020: Plaintiffs and the District agreed to pause the implementation of the DII due to the COVID-19 Public Health Emergency. During this timeframe, the Disability Coordinator held weekly and biweekly teleconferences with the DCAG to provide situational awareness of the District's response to the pandemic and learn of any unmet needs in the disability community.
- Dec 2020 – Produced the Annual Shelter Database Report.
- Dec 2020 - Produced the Annual Shelter Report of Capital Projects of District-owned Buildings.
- Dec 2020 – Produced the Post Emergency Canvassing Operations Report.

[1] Section 508 of the Rehabilitation Act requires that all website content be accessible to people with disabilities.

- Jan 2121 – Reconvened the High-Rise Building Evacuation Task Force (HRTF.) Primary support member agencies are: FEMS, DCRA, OUC, DGS, and ODR. Noteworthy: Plaintiffs' SME (Ms. Denise Grimm) sits on the HRTF, per Settlement Agreement. (Goal for this FY is to produce the High-Rise Building Evacuation Gap Analysis by August)
- Jan 2021 – Produced the HRTF Work Plan to Improve the District's Approach to Evacuating People with Disabilities from High-Rise Buildings.
- Jan 2021 – Produced the HRTF Project Management Plan.
- Feb 2021 - Produced the Transportation Needs Analysis Report.
- Feb 2021 – Held HRTF Virtual Meeting.
- Mar 2021 – Held HRTF Virtual Meeting.
- Mar 2021 – Disability Community Advisory Group First Quarter Meeting.

Interior Flood Risk Data Collection

Description: The purpose of this meeting was to strategize about the best use of public and private resources to collaborate on risk reduction programs and project delivery. Through this process, both the District and FEMA annually review risk reduction priorities, evaluate the status of reaching those priorities throughout the year, and identify the best way to leverage existing resources for implementation. As a result, District partners and FEMA can build upon the priorities identified in previous Risk Reduction Consultations.

Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: In light of 2019 findings, HSEMA prioritized the need to collect more robust interior flood risk data within the metro area specifically geared towards interior flood measures. Mitigating the urban heat island effect, such as through green roofs and social interventions like Resiliency Hubs, presents a unique opportunity to reduce both extreme heat and flood risk. While the District has set a national example in blue-green infrastructure, there continues to be a need for deeper cross-agency collaboration as some mitigation strategies overlap priority planning areas for Capital Improvement Plan, Comprehensive Plan, Resilient DC, and Climate Ready DC.

District Hazard Mitigation Plan

Description: The District Hazard Mitigation Plan (DHMP) serves as a District-wide guide for organized and coordinated efforts to mitigate the threats and hazards in the District. This Plan provides critical information, situation assessments, risk assessments, and operational tactics based on best practices to aid multi-agency efforts in mitigating District hazards, and establishes a base for thorough identification of hazards, risk analysis, efficient hazard management, and implementation of hazard reduction and avoidance measures. The mitigation strategy developed herein supports resilience through minimizing and eliminating human suffering and property loss associated with hazards and their consequential disasters.

Funding: Has a potential of at least $40M in FEMA hazard mitigation funding

through building resilient infrastructure communities and flood mitigation assistance and through a conditional amount based on the damage assessment if a disaster strikes.

Results: The District submitted grant applications including efforts to support Office of Planning (OP) comprehensive planning efforts and flood mitigation in Southwest and Watts Branch neighborhood.

Business Emergency Management Operations Center
Description: The Business Emergency Management Operations Center (BEMOC) is an alliance of public-private partners committed to improving the District's private sector's ability to prepare for, respond to, and recover from disasters. The BEMOC provides local businesses with emergency response information, planning assistance, trainings, and exercises. During FY2020, BEMOC implemented new procedures to provide timely situational updates in advance of, and during, incidents in collaboration with multiple other agencies including DMPED, DDOT, DPW, MPD, and DCRA.

Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.

Results: The BEMOC coordinated nine calls for providing updates on demonstrations, the RNC convention, elections, and more. In addition, summary emails of these calls were sent to the BEMOC list, and situational update emails were sent at other times where calls were not the most efficient way to disseminate information. This included during the 2020 November elections, when situational update emails were sent with partner agency input every eight hours over the course of several days. The BEMOC email list has grown to over three hundred contacts over the past year, and several Business Improvement Districts and other organizations have further spread these situational updates to their own lists to expand the reach of this information.

NTIC – Target Violence and Terrorism Prevention
Description: The District of Columbia (DC) is an attractive target for a variety of extremist ideologies due to the myriad of symbolic targets here. The changing nature of our threat environment poses a challenge to interceding before violence. To combat this issue, NTIC has received grant funding to develop and conduct Mobilization to Violence Awareness Training (MVAT) to at least 5,500 DC individuals involved in local law enforcement or community support—including faith-based institutions, schools, and higher education. The training is based on USDHS's Law Enforcement Awareness Briefing (LAB) and supplemented with local context approved by the MVAT Task Force—composed of subject-matter experts and partners drawn from law enforcement and our community support network. This training will help our stakeholders draw the connection between federal priorities to the local nexus. The presentations are being designed to provide attendees practical and actionable guidelines to recognize and report concerning behavior before it escalates to violence. Trainings will be crafted for in person and virtual sessions.

Funding: DHS awarded a grant to the NTIC of $150,000 that is being used to hire two contractors for the project.

Results: The contract hires are on board and have started developing training modules for the NTIC.

40. How does the agency measure programmatic success? Please discuss any changes to outcomes measurement in FY20 and FY21, to date.

HSEMA measures programmatic success through the Key Performance Indicators (KPI) and workload measures documented in the agency's performance plan. During the development of the FY21 performance plan, the language in multiple measures was modified slightly to better articulate the activity being measured. For example, the KPI "Percentage of new or revised plans…socialized through training or exercise" was modified to include both exercises and real-world events as potential mechanisms to validate plans.

Additionally, HSEMA converted two workload measures related to training into KPIs to allow for target setting and better measurement of outcomes.

41. What are the top metrics and KPIs regularly used by the agency to evaluate its operations? Please be specific about which data points are monitored by the agency.

HSEMA tracks performance primarily through the KPIs and workload measures on our performance plan, as listed below. Among the highest priority metrics that HSEMA monitors are the number of planning processes completed in accordance with the Emergency Management Accreditation Program requirements, readiness for EOC activation as measured by compliance with training requirements, and the increase in subscribers to the AlertDC program.

Please see the Key Performance Indicators and Workload Measures information, below:

Key Performance Indicators
Percentage of employees with activation responsibilities trained in their EOC role
Percentage of eligible EOC staff in attendance at EOC Readiness training per quarter
Percentage of weekly EOC facility inspections completed per quarter
Percent of distributable analytic products co-authored with one or more federal, state or local partners
Percentage increase in subscribers to fusion situational and analytic product distribution lists
Percentage of EMAP accreditation standards for which HSEMA has current documentation
Percentage of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements

Percentage of new or revised plans (where the planning process was led by HSEMA) socialized through training, exercises or real-world events.
Percentage of executive level staff with responsibilities in the Emergency Operations Plan completing an emergency senior/cabinet level training within 60 days of onboarding
Percent of District agencies with lead and support roles in the District Preparedness Framework that participated in HSEMA led trainings or exercises
Amount of competitive grant funding awarded to HSEMA for resilience and hazard mitigation
Percentage of Single Member Districts where HSEMA conducted a community preparedness training or event.
Percentage increase of recipients of AlertDC
Percentage of Grant dollars spent within the timeframe of grants
Percentage of federal subgrants issued within 45 days of award receipt

Workload Measures	
Number of level 3 (enhanced) or higher Emergency Operations Center activations	Number of raw suspicious activity reports (SARs) processed
Number of days JAHOC teams are deployed to special events	Number of requests for information (RFIs) processed
Number of AlertDC messages sent to the public	Number of community preparedness trainings or events attended or conducted by HSEMA
Number of HSEMA alerts sent to District government staff	Number of special events that have been processed by the Mayor's Special Events Task Group
Number of days agency staff are deployed to incident sites	Number of reimbursements processed for subrecipients annually
Alerts processed through JAHOC inbox	Number of active subawards
Number of District plans created, revised, or reviewed for District Government partners annually	Number of grant monitoring visits
Number of trainings provided to first responders, District employees, and the public by HSEMA	

42. Please identify whether, and if so, in what way, the agency engaged The Lab @ DC in FY20 or FY21, to date.

While staffed to the Human Services Branch of the District's COVID-19 response, and in coordination with the District Department of Human Services and the District's Office of Planning, HSEMA staff worked with The Lab @ DC to design and analyze the results of a survey distributed to community members visiting the District's grocery distribution sites during COVID response.

Additionally, in their role supporting the District's Building Blocks program, HSEMA staff work with members of The Lab @ DC assigned to the Data and Analysis group of the Gun Violence Prevention Emergency Operations Center.

43. Please list the task forces and organizations of which the agency is a member.

Locally, HSEMA manages the District Preparedness System and serves as co-chair of the District's Emergency Preparedness Committee (EPC). HSEMA is also an active participant in the following task forces and working groups:

- School Safety Alliance (formerly the Emergency and Safety Alliance);
- Resilient DC Cabinet;
- Capital Trails Coalition;
- Interagency Council on Homelessness;
- Smarter DC Tiger Team;
- Safe Passage to Schools;
- Disability Community Advisory Group and associated work;
- Disability Integration Initiative (DII) Outreach and Integration Working Group;
- DII Accessible Emergency Communications Working Group;
- DII Emergency Sheltering and Power Outage Working Group;
- DII Post Emergency Canvassing Working Group;
- DII Accessible Transportation Working Group;
- DII High-Rise Evacuation Working Group;
- DC Presidential Inaugural Committee;
- PIC;
- DC Silver Jackets;
- Resilience Hub Interagency Workgroup;
- Southwest Buzzard Point Flood Resilience Strategy Interagency Workgroup;
- National Emergency Managers Association, State Hazard Mitigation Officer's Committee;
- DC Department of Health Director's Opioid Committee;
- DC Health and Medical Coalition;
- DC Human Trafficking Task Force;
- USDHS Resilient Investment Planning and Development Work Group (RIPDWG) – currently serving as Vice Chair;
- US Secret Service Critical Infrastructure Group for National Special Security Events – currently serving as Committee member;

- US Green Building Council's LEED Green Building Advisory Committee;
- DC Alliance for Response (Foundation for the American Institute of Conservation);
- DCPS ReOpen Strong;
- Vision Zero; and
- Gun Violence Prevention Task Force.

44. Please explain the impact on your agency of any federal legislation passed during FY20 and FY21, to date, which significantly affected agency operations.

No Federal legislation passed during FY20 and FY21, to date has significantly affected agency operations.

45. Please describe any steps the agency took in FY20 and FY21, to date, to improve the transparency of agency operations, including any website upgrades or major revisions.

In an effort to improve the transparency of agency operations, HSEMA utilized Siteimprove, a web-based tool provided by the Office of the Chief Technology Officer (OCTO), to improve the 508 compliance of all pages on the HSEMA website. The agency website now exceeds the government benchmark for accessibility. Additionally, HSEMA's Information Technology Bureau, in partnership with OCTO, made updates to the HSEMA mobile application to ensure the accessibility of preparedness and emergency information for all residents.

In FY20, HSEMA also utilized the *HSEMA Off the Record* podcast, originally launched in 2019, to communicate information on District services and preparedness tips and resources available to residents. The podcast also provides a behind the scenes look into agency activations, such as HSEMA's role in the COVID-19 response and recovery efforts. HSEMA's Office of Public Affairs will continue to use the podcast in FY21 as a platform to help residents better understand the agency's role in steady state or emergency initiatives and the resources available to help them become better prepared.

46. Please identify all electronic databases maintained by your agency, including the following:

a. A detailed description of the information tracked within each system;

b. The age of the system and any discussion of substantial upgrades that have been made or are planned to the system; and

c. Whether the public can be granted access to all or part of each system.

The table below includes information on all electronic databases maintained by HSEMA.

Type	Description	Age	Upgrades	Public (Y/N)
MS SQLServer	Production WebEOC database - Application front end is utilized by District agencies and partner agencies during events	5Yr	Updated in 2020	Y
MS SQLServer	Production CORE DC database - Application front end is utilized by District agencies and public agencies during events	1Yr	Updated in 2020	Y
MS SQLServer	Database for Citywide closed-circuit television (CCTV) camera system integrated environment.	5Yr	2016	N
MS SQLServer	Redundant Database for Citywide CCTV camera system integrated environment	5 Yr.	2016	N
MS SQLServer	Production database for HSEMA Training Tracking system - Application front end available to the public	4 Yr.	2019	Y
MS SQL Server	Redundant Database for WebEOC database application and HSEMA Training	2 yr.	2020	Y
MS SQL Server	Redundant Database for CORE DC database application and HSEMA Training	1 yr.	2020	Y
MS SQLServer	Production ManageEngine ServiceDesk - Application front end is utilized by DC HSEMA for Helpdesk ticketing	6 Yr.	None	N
MS SQLServer	Production ManageEngine DesktopCentral - Application front end is utilized by DC HSEMA for Desktop Management	6 Yr.	None	N
MS SQLServer	Doubletake Database - Utilized to replicate data to OCTO DR Environment	2 Yr.	None	N

47. Please provide a detailed description of any new technology acquired in FY20 and FY21, to date, including the cost, where it is used, and what it does. Please explain if there have there been any issues with implementation.

Agency Wide Equipment Refresh
In FY20, HSEMA continued with an agency-wide workstation refresh. During this process the agency procured Dell monitors, keyboard and mice sets, and monitor stands. The procurement of the new laptops and workstations allowed the agency to replace outdated equipment and increase the agency's productivity. The cost of this agency-wide refresh was $102,231.90. This was procured with UASI grant funding.

HSEMA EOC Refresh
In FY20, HSEMA undertook an EOC refresh for EOC stations. During this process the agency procured Desktops ($118,967.00) and supporting graphics cards ($30,299.00), monitors, equipment for a mobile EOC ($77,088.66) to better support COVID activities, and MS Office licensing ($84,165.80) for this equipment. This equipment was purchased with COVID Contingency funding with the exception of the MS Office, which was UASI grant funded.

Digital Signage
In FY20, HSEMA procured a replacement for existing digital signage for the HSEMA facility. This procurement was to replace faulty and unsupported signage that was in use by the agency. This equipment allows for announcements and notifications throughout the Agency in a large screen format and is used for day to day activities and for planned and unplanned events to communicate with DC, Federal, and State ELOs activated at the agency. The total cost of this equipment was $21,451.00 and was procured with UASI grant funding.

Conference Room Reservation System
In FY20, HSEMA procured a conference room reservation system for the HSEMA facility. This procurement was to allow agency staff to integrate with current systems and book HSEMA facility conference rooms at each location and to confirm the status and schedule of each room to prevent overbooking of the facilities. This equipment allows for announcements and notifications throughout the agency and is used for day to day activities and for planned and unplanned events. The total cost of this equipment was $12,154.00 and was procured with UASI grant funding.

Dell Laptop Procurement
In FY20, HSEMA procured a number of Laptops. Specifically, the agency procured 21 Dell laptops in order to facilitate the JAHOC Operations staff remote efforts due to COVID-19 telework requirements ($38,593.80), 20 Dell laptops to support Inauguration activities and the DC PIC Office ($37,215.80), and 20 Dell laptops to support newly onboarded HSEMA staff and replace out of date equipment ($42,615.80). JAHOC laptops were purchased with COVID funding, the Inauguration laptops were purchased with Inauguration funding, and the remainder were purchased with UASI grant funding.

Webex Board Infrastructure
In FY20, HSEMA procured Cisco Webex Board equipment for agency conference facilities. These boards allowed for staff at HSEMA headquarters to seamlessly connect to the COVID EOC activated out of DC Health's HECC throughout most of 2020. These boards operate in a conference environment allowing users to wirelessly present, whiteboard, video, and audio conference for events. These boards were used by HSEMA and other DC agencies to share content and provide conferencing facilities during the COVID response and other events surrounding Inauguration and will continue to be used in a similar manner. This allows HSEMA to support a socially distanced workplace environment for all ELOs now and in the future. Equipment that was procured included three Cisco Room Kits, two Cisco Webex 55" Boards, three Cisco Webex 70" Boards and 11 Cisco Webex Desktop boards for a total of $191,631.90. This equipment was purchased with COVID Contingency funding. This type of equipment has been heavily invested in by OCTO and HSEMA has worked with OCTO on the rollout of this equipment.

JIRA Team Management Software
The JIRA application was procured by HSEMA in preparation for the new CORE DC development in 2020. The $4,500 cost of this software was procured with UASI funding and provides 50 users for a one-year term. It was determined that a number of different development teams would be required for this effort both internal and externally to HSEMA. JIRA is a tool that manages the work of software development teams from requirements through development, testing and production release. JIRA was used heavily during the response and building of WebEOC and CORE DC for the COVID response, in particular for the building of Resource Request management for the District. It is successfully being used by the agency and will be used as development continues into 2021.

Agency Specific:

48. Please discuss how the public health emergency related to COVID-19 affected agency operations during FY20 and FY21, to date.

COVID-19 required an all-hands response for the agency from March 2020, continuing into the present. This means that all agency staff were/are either fully engaged in the response in the Emergency Operations Center (EOC) or they were/are specifically reserved from the response to execute the agency's mission essential functions. Notably, our staff operated the District's EOC from the DC Department of Health to be collocated with DC Health's COVID-19 operations.

For months – the longest sustained emergency activation of the EOC in District history – our staff dedicated all of their working hours to coordinating and supporting this unprecedented effort that integrated every aspect of the District's considerable resources. Our enduring objectives were to slow the spread of COVID-19, provide human services support to impacted community members, and sustain or curtail essential government services. HSEMA assigned staff – often whole teams – to every aspect of the operation.

As a result of this all-hands response, HSEMA has had to balance efforts on previously ongoing initiatives. Of our ongoing initiatives, we focused on (1) sustaining our regional grants management administration, (2) improving the EOC and administrative information management systems, and (3) rolling out new, online models for emergency management training and education.

Notably, COVID was only one of the incidents for which HSEMA coordinated response operations across all District government agencies. Others in FY20 and FY21, to date included:

- Washington Nationals World Series Championship and Parade
- Sustained summer heat emergencies with heavily modified operations for COVID physical distancing
- Modified July 4th activities and support to community COVID-reduction interventions
- Civil unrest following the death of George Floyd
- Lying-in-state of Supreme Court Justice Ruth Bader Ginsburg
- Tropical Storm Isaias
- Severe localized flooding on Sept 10
- Million MAGA March
- 2020 Presidential Election
- Insurrection and siege of the US Capitol building on Jan 6
- 2021 Presidential Inauguration
- Snow/Winter Weather Response

49. Please describe, with specificity, the agency's role in the COVID-19 response and the related public health emergency.

a. What has HSEMA learned from its role in the last eleven months that inform its current and future operations and planning?

As noted above, COVID-19 required an all-hands response for the agency from March 2020 to the present time. Thus, all agency staff are either fully engaged in the response in the Emergency Operations Center (EOC) or they are specifically reserved from the response to execute the agency's mission-essential functions.

This incident triggered the longest sustained emergency activation of the EOC in District history and our staff dedicated all of their working hours to coordinating and supporting this unprecedented effort that integrated every aspect of the District's considerable resources. Our enduring objectives were to slow the spread of COVID-19, provide human services support to impacted community members, and sustain or curtail essential government services. HSEMA assigned staff – often whole teams – to every aspect of the operation.

There is no aspect of the COVID-19 response in which HSEMA was not intimately involved. Director Rodriguez served as the Incident Commander, leading an incident management team of executive leaders to oversee and execute the COVID response. Under Director Rodriguez's leadership, the majority of HSEMA's staff stepped into critical roles to coordinate the operation.

- **Executive Team.** In addition to Director Rodriguez, HSEMA provided the Planning Section Chief and the Deputy Operations Section Chief for the Mayor's executive incident management team.
- **Emergency Operations Center (EOC).** At the direction of the Mayor, HSEMA established the EOC at 899 North Capitol St, jointly located with DC Health's Health Emergency Coordination Center (HECC). HSEMA staff served in key roles throughout the EOC. The EOC provided the coordination between all District agencies and community partners to ensure that there was unity of effort to achieve approved objectives. In addition to developing daily, weekly, and monthly operational plans to unify the COVID response, the EOC implemented a process called "single point ordering" in which all procurement for disaster-related resources went through a single approval and ordering process. This process – coordinated with OCP – ensured that procurements were properly routed through the emergency procurement process and limited duplicate ordering. FEMA identified our single point ordering system as a national best practice because it allowed the District to rapidly submit disaster reimbursement requests – faster than any other state in our region. The EOC also coordinated resources to meet incident needs across all facets of the incident.
- **Joint Information Center (JIC).** Our Chief and Deputy Chief of External Affairs and Policy served as deputy Joint Information Center (JIC) managers in our long-standing role supporting EOM Comms. In this role, our team established the messaging protocols for the EOC and provided messaging, oversight, review, and publication support for every aspect of the COVID response. At the height of COVID response – and the unrelated emergencies throughout the year – we had up to five other staff supporting the JIC.
- **Field Operations Leadership and Support.** HSEMA assigned teams from the EOC to lead and support all aspects of the COVID response. Before COVID was a household term, our Operations Division had staff embedded with DC Health's incident management team. As the action picked up, our Preparedness Division staff integrated into the health and medical operations – in support of DC Health - including filling targeted roles such as: evaluating the District's healthcare facilities to expand bed counts; developing the alternate care site's internal management structures; and developing tools for patient tracking at the site. HSEMA's Chief of Homeland Security and Intelligence served as the head of the fatality management branch and set up the field morgue with OCME. We also rotated staff through the human services branch to establish a COVID-only human services warehouse with tremendous support from DGS.
- **Disaster Logistics**. Establishing the EOC required a significant number of staff to support the information technology, food services, facilities, delivery, and other operational needs. During COVID, HSEMA staff provided all of these services but did it for the largest EOC activation ever executed with the added complexity of COVID sanitation protocols. At any given time, HSEMA had 10-15 people assigned to the logistics operations, supporting the work at the EOC facility and supporting the larger mission support section led by ACA Jay Melder.
- **Intelligence and Information Support**. Throughout the activation our Fusion Center staff rotated through the EOC to support with threat evaluation, incident planning, and preparing the recurring briefings that the EOC generated on a variety of topics.

a. What has HSEMA learned from its role in the last eleven months that inform its current and future operations and planning?

Two years ago, HSEMA began to evaluate the District's capacity to manage a billion-dollar disaster, something that was almost unimaginable in scope and impact. During that process, we identified several key areas that would, if implemented, improve our ability to manage a disaster of that size.

First, we recognized that HSEMA – as an agency of 142 FTEs – was not large enough to manage an incident of that size and scope. Under Mayor Bowser's leadership, we activated deputy mayor and department head level personnel into the Mayor's executive incident management team to provide an executive layer to the response. This led to faster execution around critical issues like carefully modifying government operations. DC Government and allowed the EOC to focus on the necessary procedural activities of disaster management. DCHR also detailed staff to the EOC to expand our staffing. Notably, we continued our internship program throughout the activation and our interns have been critical to our success; indeed, several stayed on for a second or even third session when their schools transitioned to remote operations and a number have moved into career positions at HSEMA and DC Health.

Second, we identified a number of key actions that must be implemented early in the disaster in collaboration with key partner agencies to ensure that we were properly accounting for costs from the start of the incident. With support from OCTO and DCHR, we established a disaster charge code in PeopleSoft, and we implemented single-point ordering for disaster-related resources with OCP. These early steps allowed us to consolidate costs and rapidly seek FEMA grant reimbursement for eligible disaster costs.

Third, we recognized that we may have to manage other incidents even while we sustained a massive emergency response posture. As described in question 48 above, COVID was just one of the many incidents and emergencies that the District faced this year. Early in COVID, the EOC staff began to design a solution to this and established a process to assign teams to each incident as they occurred. Each team would coordinate under the overall auspices of the EOC and could reach into any agency necessary for that incident. Critically, this meant that the EOC could provide Director Rodriguez with a roll-up of activities across all incidents and he could transfer that to the Mayor's executive incident management team as a consolidated report each day during regular briefings.

Fourth, we recognized through recurring planning with FEMA that the District had several key limitations with regards to Disaster logistics, specifically resource staging and warehousing. Under the leadership of ACA Melder, OCP Director George Schutter, and our partners at DPW and DGS, the District's disaster warehousing capacity rapidly expanded to six warehouses to house our PPE, sanitizing supplies, and critical equipment. Notably, HSEMA now manages a

50,000 square foot warehouse that currently supports COVID operations but will eventually transition to an all-hazards warehouse to support all manner of emergencies.

50. Please describe the mission of the Fusion Center and its activities during FY20 and FY21, to date.

a. To what extent do the Fusion Center's activities differ from those of its counterparts in other jurisdictions?

The Fusion Center solicits for and fulfills requests for analysis from public and private partners regarding emerging threat trends. The NTIC processes Suspicious Activity Reports and incorporates that information not only into investigative packages submitted to MPD and other LE agencies but leverages that information to identify changes in the threat environment. Although we are unfamiliar with the daily activities of the other fusion centers, the NTIC uniquely prioritizes joint strategic production with our partner agencies. In FY20 the Fusion Center authored 58 pieces of unique intelligence analysis For Official Use Only (FOUO) Law Enforcement Sensitive (LES), and over 600 situational awareness or officer safety-oriented products (BOLOs etc.). The NTIC hosts a successful liaison program that focuses on engagement to develop standing information needs and generate key intelligence questions to drive both collection and future analysis. The District Fusion Center was the only regional center to support COVID-19 operations and future planning and analysis within the EOC, and it maintains analyst support for that effort still.

b. What is the Fusion Center's relationship to hate crimes? The possession of illegal firearms?

The Fusion Center supports information sharing associated with hate crimes when identified through posts of concern or when they are submitted as a suspicious activity report. The Fusion Center manages information sharing regarding illegal firearms when identified with potential terrorist activity such as weapons acquisition.

51. How did HSEMA promote awareness among the District's public and private sector partners regarding cybersecurity in FY20 and FY21, to date?

The NTIC Cyber Center produced almost 100 cyber bulletins, alerts, and briefings sharing to both public/private entities.

52. How does HSEMA ensure collective situational awareness and coordination among District agencies, including independent agencies, and federal partners in the area of cybersecurity?

a. What cyber awareness outreach and training did HSEMA conduct in FY20 and FY21, to date?

As a result of the COVID-19 outbreak, outreach and training was limited to internal staff instruction and engagement only.

53. Please describe the activities of the Homeland Security Commission in FY20 and FY21, to date.

The HSC, under the leadership of Chairman Belzak, was extremely active and held several virtual meetings throughout the pandemic. The HSC completed its 2020 annual report, which was submitted to Council in early February 2021. The Commission's next quarterly meeting is set for early March, where they will hone their next study topic.

a. What is HSEMA's plan for reviewing and implementing the core recommendations of the Commission's 2020 report, "Emergency Mass Care Programs Across the Nation: Best Practices for the District", particularly when they cut across agencies, such as:

- ***Consider performing a mass care and sheltering capabilities assessment***
- ***Evaluate and revise sheltering and mass care plans for operating in a COVID-19 environment***
- ***Consider creating a "Mass Care Working Group"***
- ***Consider developing a "Mass Care Technology Advisory Council"***
- ***Consider creating a "Disaster Rapid Assessment Team", led by HSEMA, to focus on improving District mass care services ahead of an emergency event***

HSEMA is currently reviewing the HSC's 2020 report on mass care and plans to work closely with the Department of Human Services (DHS) and other key partner agencies to implement the report findings. Since the HSC report identified best practices from emergency mass care programs outside the District, we are currently evaluating those practices against our current programs so we may identify opportunities to bolster our programs ahead of an emergency event.

54. How did HSEMA improve collective situational awareness and coordination among District agencies and District residents in the event of a mass emergency in FY20 and FY21, to date?

a. How has HSEMA changed its operations or coordination with relevant public and private entities following the Capper Fire? How has HSEMA used its "lessons learned" from that event to inform agency operations?

One of the major improvements from the Capper Fire is the implementation of the District's Residential Displacements protocol. Under this protocol, as soon as any agency notifies the District's Joint All Hazards Operations Center (JAHOC) that an incident is going to trigger displacements of a large residential building – like the Capper Building – the JAHOC issues a targeted notification to all of the agencies that may have a responsibility to support the community. The JAHOC then deploys a staff

member to the site and the staffer evaluates the incident. The JAHOC continues to provide email updates to the Residential Displacements Group and, if necessary, sets up a series of conference calls for the group to assess and support the community. The calls continue until the displaced residents relocate themselves or are safely relocated to a hotel and connected to ongoing support services from District government agencies, such as OTA, DHS, and DHCD.

More generally, HSEMA has also increased the number of staff that can deploy to an incident site 24 hours a day. For example, at a fire with a large evacuation and then displacements on G St SW, HSEMA sent five staff out late in the event to assist tenants with recovering their belongings and transiting to hotels. We have also continued to expand our Mobile Situational Awareness Teams (MSAT) that deploy throughout the District during incidents and events to gather "eyes on" information to identify impacts to District operations and provide logistical support to other District agencies. For example, during the modified July 4th festivities, HSEMA's MSAT teams traveled all over the District to monitor for crowds and deliver supplies to violence interruption efforts in all 8 wards. Our MSATs were instrumental in gathering on the-ground situational awareness during every major incident in FY20 and FY21, to date, including the protests following the death of George Floyd, the January 6th Insurrection, 2020 Elections and 2021 Inauguration.

b. Did HSEMA conduct any tabletop exercises or drills to practice how to respond to future large-scale events? If so, please explain.

COVID required us to find new and innovative ways to manage incidents – specifically to augment our face-to-face situational awareness practices with new technology. During COVID, we leveraged web-based tools like Microsoft Teams and Cisco's WebEx platform to conduct virtual meetings and share information between operating centers. In preparing for Inauguration, HSEMA developed a WebEx network that connects the EOC to the District's various department operations centers so that staff who would traditionally go to the EOC could continue to collaborate face-to-face from their own operations centers. This included developing a training curriculum and conducting a series of exercises before using the system for all of the events leading up to Inauguration and the Inauguration itself.

c. Did HSEMA change any internal policies on how it responds to large-scale events? Specifically, with regard to its responses to vulnerable populations, such as seniors or individuals with disabilities? If so, please outline these changes.

HSEMA collaborates with organizations that represent vulnerable populations in the District. HSEMA continues to review and improve our emergency response plans to meet the needs vulnerable populations. HSEMA has not made significant internal policy changes how to address vulnerable populations during large scale events.

55. Please provide an update on Alert DC during FY20 and FY21, to date.

a. How does the agency track the number of subscribers? How has this number changed over the past two fiscal years?

HSEMA tracks AlertDC subscribers through Everbridge, the platform powering AlertDC. HSEMA achieved significant growth in public subscribers and attributes this growth to the agency's commitment to public education and awareness campaigns. In FY20, the agency launched four AlertDC public awareness campaigns and experienced a 493% growth with nearly 72,750 new subscribers. In contrast, the agency gained approximately 14,700 new subscribers in FY19 and 3,600 new subscribers in FY18.

b. How has this program been used to communicate important information?

During FY20, AlertDC was used to communicate 9,678 alerts to subscribers. Alerts range widely in topic, for example: silver alerts, emergency water outages, traffic advisories, street closures, special event information, and hypothermia/cold emergency alerts. AlertDC was also used to communicate critical updates to District residents and businesses throughout the COVID-19 pandemic.

So far in FY21, AlertDC has sent approximately 862 alerts.

c. What does the agency believe it the appropriate use of the program to inform residents living near the U.S. Capitol Complex concerning timely and relevant security and public safety information, particularly when the U.S. Capitol Police does not share such information?

AlertDC is the official District of Columbia communications system allowing residents and visitors to pick the type of emergency alerts, notifications, and updates directly from the District of Columbia's public safety officials. AlertDC messages are deployed by the District's Joint All Hazard Operations Center (JAHOC) with information coming from local, regional, and federal partners.

56. Please provide a list of all major special events that HSEMA monitored in FY20 and FY21, to date.

- Major League Baseball World Series (7 Games)
- Nationals World Series Victory Parade
- 2020 State of the Union Address
- Independence Day 2020
- 59th Presidential Inauguration

a. Please describe how the agency responded to each event.

For all listed events, HSEMA increased the activation level of the EOC to provide enhanced operational coordination, situational awareness, and resource support, and deployed mobile situational awareness teams. For the 2019 MLB events and

Independence Day 2020, HSEMA also deployed the mobile command vehicle to the event sites to maintain situational awareness and provide onsite coordination.

57. How did HSEMA improve its engagement with the Council in FY20 and FY21, to date?

Providing accurate and timely answers to inquiries from Council is a top priority for HSEMA. Several members of the HSEMA staff are tasked with tracking Council actions and responding to requests from Councilmembers. In addition, Councilmembers are encouraged to sign up for AlertDC to receive timely notifications about activities throughout the city. Further, the agency continues to work closely with the Mayor's Office of Policy and Legislative Affairs (OPLA) on any outstanding concerns from Council.

a. In an emergency situation, what is the formal protocol for notifying members of the Council about HSEMA's response plans?

HSEMA encourages all Councilmembers to sign up for AlertDC to customize the alerts that they receive on a daily basis. In addition, during larger scale emergencies that include level 2 or higher activation of the Emergency Operations Center, the Joint Information Center's (JIC) Legislative Affairs Unit is responsible for communicating with Council. During multi-day activations, the JIC hosts a daily call for Councilmembers and staff to update them on the District's response.

b. How can HSEMA and the Council work together to help keep constituents informed and apprised of important information?

HSEMA encourages the Council to promote AlertDC (alertdc.dc.gov), the District's emergency communications system, to constituents. We would also encourage Council to promote ReadyDC (ready.dc.gov), the District's personal preparedness campaign, in its constituent communications and urge residents to sign up for the ReadyDC Preparedness Bulletin (ready.dc.gov/bulletin). The Preparedness Bulletin is an electronic newsletter that shares preparedness news, resources, trainings, and tips with the community. ReadyDC asks residents to become a preparedness partner by being aware, making a plan, building a kit, and staying informed. Finally, Council is also encouraged to contact members(s) of HSEMA's community outreach team for presentations on emergency preparedness and printed preparedness resources by visiting hsema.dc.gov/communityoutreach.

In FY19, HSEMA worked with Councilmembers to modify the language of AlertDC messages based on feedback Council received from constituents. We continue to welcome the feedback of Councilmembers and their constituents to ensure that emergency messages and alerts are clear and actionable.

During the COVID-19 response, the Executive Office of the Mayor participated in daily (and then transitioned to weekly) conference calls with members of Council to share important information related to the District's response. Now weekly, these calls

provide an opportunity for Council to pre-submit questions related to various aspects of the response and an opportunity to help communicate critical information to residents.

58. Please describe the structure, membership, and responsibilities associated with the Mayor's Special Events Task Group ("MSETG").

As the nation's capital, Washington, D.C. hosts numerous special events requiring essential municipal services to ensure events occurring on public roadways in the District are conducted in a manner that protects public health and safety. Coordinating the city's interagency public safety planning efforts is the responsibility of the Mayor's Special Events Task Group (MSETG). The MSETG's structure is based on the functional areas of responsibilities listed below in support of the city's two special event licensing and permitting agencies (i.e., MPD for processional events and DCRA for stationary events).

Functional Area(s) of Responsibility	Lead Agency
Security	Metropolitan Police Department
Transportation, Public Space, and Public Works	Department of Transportation *and* Department of Public Works
Licensing, Permitting, and Inspections	Department of Consumer and Regulatory Affairs
Health and Medical	Department of Health *and* Fire and Emergency Medical Services Department
Unified Command and Communications	Homeland Security and Emergency Management Agency

In order to ensure effective deliberation and working representation of agencies with primary and supporting functions, the MSETG's membership includes the following:

MSETG Membership	
Homeland Security and Emergency Management Agency	Department of Consumer and Regulatory Affairs
Department of Fire and Emergency Medical Services	Alcoholic Beverage Regulation Administration
Metropolitan Police Department	Office of Risk Management
District Department of Transportation	Department of Health
Executive Office of the Mayor	Department of Public Works
DC Water	Office of Tax and Revenue

National Park Service	Department of Parks and Recreation
Washington Metropolitan Area Transit Authority	Office of Cable Television, Film, Music, and Entertainment
Events DC	Smithsonian Institute
U.S. Park Police	U.S. Capitol Police
U.S. Department of Homeland Security – Federal Protective Service	Department of General Services Protective Services Division
National Gallery of Art	Department of Energy and Environment

a. Please describe the work of the MSETG in FY20 and FY21, to date, including any changes to its reporting structure within the Executive branch, membership, operations, policies, procedures, and member agency fees.

The MSETG held semi-monthly meetings during FY20 and FY21, to date, for the purpose of providing interagency reviews and assessments of the operational, public safety, and logistical components of proposals for special events occurring on public roadways under the jurisdiction of the District of Columbia. The Meeting Activity Report (attachment "Q58a HSEMA part 1") provides a list of the event proposals reviewed and assessed by the MSETG for production during FY20 and FY21 Q1. The MSETG's reporting structure within the Executive Branch remains under the Executive Office of the Mayor (via the Mayor's Office of Community Affairs). There were no changes to the MSETG's membership, operations, or procedures. The infographic of the MSETG's interagency coordination (attachment "Q58a HSEMA Part 2") provides an overview of the steps involved in the processing of special event proposals. Information relative to agency-specific requirements and fees is provided in the MSETG Special Events Planning Guides (attachments "Q58a HSEMA Part 3" for 2020 and "Q58a HSEMA Part 4" for 2021).

The special event user fees as determined by each respective agency incurring costs associated with the production of special events are provided in the MSETG Planning Guide beginning on page 32.

b. Please describe the reason for any fee increases in FY20 and FY21, to date (*if necessary, to answer the question, consult with agency partners*).

The MSETG does not have a role in the determination or the assessment of agency-specific special event user fees. MPD, however, reported a three percent fee increase in both FY20 and FY21 in accordance with 24 DCMR § 720.

c. Does the MSETG require event organizers to submit after-action reports once their event is complete? How is an organizer's performance taken into consideration in a subsequent application?

The MSETG encourages event organizers to submit after-action reports subsequent to the production of their events. The submission of an after-action report is used as a method of documenting key successes and determining areas of improvement for future planned productions of events.

When there are issues or problems identified in an after-action report or during an event, event organizers are required to participate in after-action meetings with the MSETG to establish action items and implement measures that will specifically address identified deficiencies prior to the MSETG's consideration of the event for approval in a subsequent year.

d. What new requirements did the MSETG or its member agencies impose upon event organizers in FY20 and FY21, to date, related to homeland security concerns (*e.g.* sandbags, placement of vehicles to block access)?

Due to the Public Health Emergency, the District of Columba has issued an emergency order banning mass gatherings, which led to many events that the MSETG managed to be significantly reduced or in most cases canceled in FY20 and FY21.

59. How did HSEMA adapt its operations in FY20 and FY21, to date, to account for increased development in waterfront areas and increased use of the water itself? Did HSEMA play a coordinating role for other District government agencies on waterfront issues? If not, why not?

During FY 20, HSEMA, a member of the DC Silver Jackets (co-chaired by DC Department of Energy and Environment (DOEE) and the U.S. Army Corps of Engineers (USACE)), contributed toward technical review of the Buzzard Point feasibility study commissioned by DDOT. Although the study is underway, there is a need to engage federal partners in the vicinity to invest in strengthening resilience in the floodplain. Additionally, through Silver Jackets, HSEMA awarded approximately $150,000 in FEMA funding to support the Office of Planning's (OP) comprehensive planning efforts and stakeholder coordination in support of long-term flood reduction in SW. In FY21, coordination of the previous effort involved HSEMA, OP, and others in applying for a $24 Million FEMA grant to mitigate stormwater flooding along the First Street SW corridor, between Lansburgh and King Greenleaf Park using resiliency measures (blue/green infrastructure).

60. Please discuss any changes the agency made to COOP planning in FY20 and FY21, to date, including preparing for the implementation of B23-0542, the "District Government Continuity of Operations Plans Amendment Act of 2020".

HSEMA has made several changes to the District's COOP program to prepare for implementation of the new legislation:

- HSEMA began requesting that agencies designate a backup COOP Coordinator in FY20. This will now be required of agencies as a result of the new COOP

legislation. Thirty-four of 42 cabinet-level agencies have designated a backup COOP Coordinator.

- A major initiative in FY20 was to build out a new online emergency management platform, CORE DC. In October 2020, HSEMA first introduced CORE DC to internal users, and debuted the COOP section for agencies in November. Among other features, this online platform will serve as a repository of information on agency locations, POCs, functions, and more. Designation of a backup COOP Coordinator is a required element of CORE DC for each agency. HSEMA has developed training modules to assist agency COOP Coordinators and backups with navigating this new system.
- Independent agencies were not required to complete a COOP plan under Mayor's Order 2012-61. The new COOP legislation extends the requirement to these agencies, and thus these agency profiles have been set up in CORE DC and prepopulated by HSEMA with the addresses of the District's real estate portfolio and a database of each agency's functions to reduce the workload of individual agencies to complete COOP requirements.
- Among independent agencies, 23 have now designated COOP Coordinators, 12 have identified a backup COOP Coordinator, and 8 provided an updated COOP plan in 2020.
- The 2020 annual COOP progress memo was sent to the City Administrator and Councilmember Allen, as the Chairperson for the DC Council committee overseeing HSEMA. This is a new requirement in the COOP legislation, in addition to the memo being sent to the Deputy Mayor for Public Safety and Justice included in both the Mayor's Order and the legislation. This memo also included the designation of a District COOP Program Manager, Tony Goodman, as required in the legislation.

61. Please describe the activities of HSEMA's Interfaith Preparedness and Advisory Group in FY20 and FY21, to date, particularly since the late spring of 2020.

The Interfaith Preparedness and Advisory Group (IPAG) mission is to provide a platform for Faith-Based Organizations (FBO) to exchange information among themselves and with District Agency representatives concerning threats, vulnerabilities, best security practices, and protective measures related to the safety and security of their congregations and facilities. The IPAG is sponsored by the Mayor's Office of Religious Affairs, HSEMA, and MPD. The IPAG provides a platform for faith-based organizations to exchange information with security and preparedness professionals on threats, vulnerabilities, best security practices, and protective measures related to the safety and security of congregations and facilities. The following list of events took place with the IPAG members during 2020.

Event	Date/Time
Security Houses of Worship- workshop- DHS (In Person)	Thurs. March 12, 2020 at 7pm
Grief and Loss in the Time of COVID-19 Training Session (virtual)	Mon. April 27, 2020 at 1pm
COVID-19 - Phase Two Reopening Clergy Webinar (Virtual)	Wed. June 24, 2020 at 1pm
COVID-19 - Phase Two Best Practices Call (Virtual)	Wed. July 1, 2020 at 1pm

Interfaith Preparedness and Advisory Group and DC Clergy Call -Preparing Faith Community for the events of Jan 6th (virtual)	Mon. January 4, 2021 at 1pm
Multi-Stakeholder Emergency Preparedness Call (virtual)	Fri. January 15, 2021 at 4:30pm
COVID-19 Vaccine 101: A Discussion with Clergy (virtual)	Fri. January 29, 2021 at 2pm

a. Does the agency maintain an updated contact list of faith institutions in the District? How does the agency ensure that faith institutions are able to access timely and relevant information and maintain points of contact within the agency?

HSEMA regularly updates a distribution list that currently has over 130 faith-based institutions. HSEMA monitors an IPAG email address and collaborates with points of contact within the NTIC to maintain steady flows of information between the agency and those institutions.

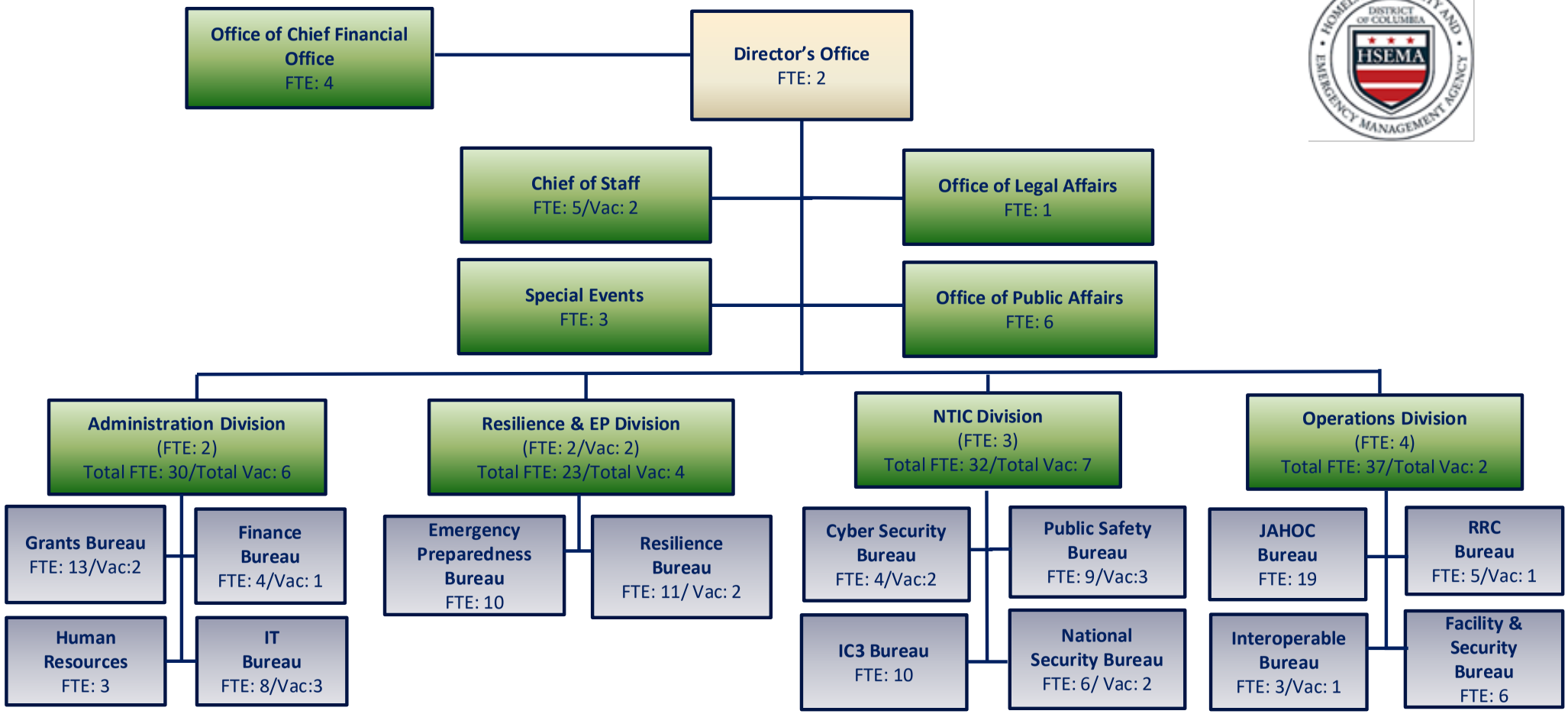
b. What grants did HSEMA make to faith institutions in FY20 and FY21, to date, and for what purposes?

The USDHS/FEMA Nonprofit Security Grant (NSGP) is the one program we administer that specifically provides funding to enhance security at targeted nonprofit organizations, and the vast majority of those are either houses of worship or educational/cultural facilities associated with a religious group. The grants and subawards are included in our responses to question 14.

Below are the grant awards for FY19 and FY20 NSGP – the FY19 grant was received before the FY20 fiscal year started, so that grant award is not in the response to question 13, but the subawards were included in the response to question 14, as they were awarded after FY20 started.

Grant	Award
2020 NSGP	4,084,014
2019 NSGP	4,449,845

FY 2021 Organizational Chart



Agency Count: **142**
Filled: 121
Vacant: 21
As of January 31, 2021

Homeland Security and Emergency Management Agency
FY 2021 SCHEDULE A

Q2 HSEMA

Vacancy Status	FTE
Filled	121.00
Vacant	21.00
Total	**142.00**

Agency Code	Fiscal Year	Program Code	Activity Code	Filled, Vacant or Frozen	Position Number	Position Title	Employee Name	Hire Date	Grade	Step	Salary	Fringe	FTE	Reg/Temp/ Term	Filled by Local/Federal Law
BN0	21	1000	1306	F	00023160	Public Affairs Specialist	Johnson,Robyn T	4/18/2006	13	7	113,104.00	25,900.82	1.00	Reg	Local/Federal
BN0	21	1000	1306	V	00039667	Program Analyst			15	0	142,769.00	32,694.10	1.00	Reg	Local/Federal
BN0	21	1000	1306	F	00077090	Executive Assistant	Crawford,Elijah A	12/3/2012	13	6	101,758.00	23,302.58	1.00	Reg	Local/Federal
BN0	21	1000	1306	F	00085113	Program Analyst	Mena,Rebekah J.	3/30/2020	12	10	97,375.00	22,298.88	1.00	Term	Federal
BN0	21	1000	1306	F	00094706	Policy Manager	Peckumn,Nicole	2/20/2018	15	0	158,010.00	36,184.29	1.00	Reg	Federal
BN0	21	1000	1309	F	00085185	Policy Advisor	Smith,Emile C.	11/9/2020	13	6	101,758.00	23,302.58	1.00	Term	Federal
BN0	21	1000	1310	F	00012886	Emergency Management Program O	Mitchell,Tanya L	8/26/1992	14	9	130,217.00	29,819.69	1.00	Reg	Local/Federal
BN0	21	1000	1310	F	00075241	Program Analyst	Adams,Nikelle L.	10/6/2014	12	6	95,111.00	21,780.42	1.00	Reg	Local/Federal
BN0	21	1000	1310	F	00095314	STAFF ASSISTANT	Harrell,Shontae	6/25/2018	12	5	85,570.00	19,595.53	1.00	Term	Local/Federal
BN0	21	1000	1320	F	00043481	Director, Homeland Sec. & EMA	Rodriguez,Christopher Ryan	10/23/2017	PS2	0	232,693.25	53,286.75	1.00	Reg	Local/Federal
BN0	21	1000	1320	F	00048774	Deputy Director	Speranza,Carrie	11/14/2016	16	0	177,000.00	40,533.00	1.00	Reg	Local/Federal
BN0	21	1000	1320	F	00071851	Supv Mgmt and Program Analyst	Shackelford,Jerica D	8/30/2010	14	0	140,000.00	32,060.00	1.00	Reg	Local/Federal
BN0	21	1000	1320	F	00088355	Emergency Operations&Info Spec	Wilson,Larae Mechelle	3/21/2016	11	10	85,784.00	19,644.54	1.00	Reg	Local/Federal
BN0	21	1000	1325	V	00088691	Program Coordinator (State)			14	0	112,111.00	25,673.42	1.00	Reg	Federal
BN0	21	1000	1325	F	00092023	Program Coordinator (State)	Ruesch,Emily	2/21/2017	14	8	137,255.00	31,431.40	1.00	Term	Federal
BN0	21	2000	2100	F	00048765	Grants Program Manager	Alsop,Vermecia R	1/21/2009	13	7	113,104.00	25,900.82	1.00	Reg	Local/Federal
BN0	21	2000	2100	F	00075237	Plans and Preparedness Officer	White,Patrice N	2/1/1988	15	0	150,138.47	34,381.71	1.00	Reg	Local/Federal
BN0	21	2000	2102	V	00020270	Chief Resilience Officer			16	0	159,396.00	36,501.68	1.00	Reg	Local/Federal
BN0	21	2000	2102	V	00094707	Supv Mgmt and Program Analyst			14	0	129,411.00	29,635.12	1.00	Reg	Local/Federal
BN0	21	2000	2103	F	00001494	Trng. & Emerg. Exer. Officer	Quarrelles,Jamie C	6/6/1992	14	7	133,663.00	30,608.83	1.00	Reg	Federal
BN0	21	2000	2103	F	00044868	Emergency Planning Specialist	Williams,Ladona R.	6/24/2002	9	8	67,578.00	15,475.36	1.00	Reg	Federal
BN0	21	2000	2103	F	00047128	Comm Emerg Trng & Exercise Spe	White,Lisa L.	5/20/2013	12	6	95,111.00	21,780.42	1.00	Reg	Federal
BN0	21	2000	2103	F	00073462	National Incident Management S	Harrison,Leslie C	5/3/1982	13	7	113,104.00	25,900.82	1.00	Term	Federal
BN0	21	2000	2103	F	00077540	PGM ANALYST	Goodman,Anthony T.	4/13/2020	13	10	122,227.00	27,989.98	1.00	Term	Federal
BN0	21	2000	2103	F	00086315	Program Manager	Worrell,Andrew	7/11/2016	13	9	110,191.00	25,233.74	1.00	Term	Federal
BN0	21	2000	2103	F	00097102	Emergency Planning Specialist	Maury,Patrick	6/8/2020	9	10	71,106.00	16,283.27	1.00	Term	Federal
BN0	21	2000	2103	F	00097103	Emergency Planning Specialist	Mattingly,Madison	5/26/2020	9	10	71,106.00	16,283.27	1.00	Term	Federal
BN0	21	2000	2104	V	00094712	Community Outreach Specialist			13	0	94,858.00	21,722.48	1.00	Reg	Federal
BN0	21	2000	2113	F	00077972	Training and Emergency Exercis	Stewart,Jonathan	2/21/2017	14	0	149,350.00	34,201.15	1.00	Reg	Local/Federal
BN0	21	2000	2113	F	00001055	Emergency Exer. & Trng. Spec.	Cryan,Travis	8/19/2019	12	6	95,111.00	21,780.42	1.00	Term	Federal
BN0	21	2000	2113	F	00092268	Emergency Planning Specialist	Alexander,Daniel K.	9/30/2019	9	10	71,106.00	16,283.27	1.00	Term	Federal
BN0	21	2000	2134	F	00044864	Critical Infrastructure Spec	Scott,Mark	5/15/2017	14	7	133,663.00	30,608.83	1.00	Term	Local/Federal
BN0	21	2000	2306	F	00016263	Community Outreach Specialist	McCall,Kimberly	4/18/2006	13	7	113,104.00	25,900.82	1.00	Reg	Federal
BN0	21	2000	2306	F	00075242	Community Outreach Specialist	Cruz,Joiner C	1/26/2004	11	8	81,508.00	18,665.33	1.00	Term	Federal
BN0	21	2000	2306	F	00075246	Community Outreach Specialist	Brannum,Robert V	7/11/2011	6	0	103,321.71	23,660.67	1.00	Reg	Federal
BN0	21	2000	2308	F	00085186	Program Coordinator	Scott,Delores	11/2/2015	14	10	133,537.00	30,579.97	1.00	Term	Federal
BN0	21	2000	2308	V	00094705	Program Analyst			11	0	66,542.00	15,238.12	1.00	Reg	Federal
BN0	21	3000	3100	F	00007419	EMERGENCY OPERATION INFO SPEC	Hackney,David	8/15/1987	11	8	81,508.00	18,665.33	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00007835	Emergency Operations&Info Spec	Whalen,Frances E	8/5/2019	11	5	75,094.00	17,196.53	1.00	Term	Local/Federal
BN0	21	3000	3100	F	00010514	Emergency Operations&Info Spec	Wiggins Sr.,Brian	1/22/2018	11	5	75,094.00	17,196.53	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00010666	Emergency Operations&Info Spec	Rogers,Janeshia N	5/28/2019	9	4	60,522.00	13,859.54	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00011442	Supvy Emerg Oper & Info Spec.	Harley,Stephanie N	12/16/2013	12	0	91,927.50	21,051.40	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00015760	Emergency Operations&Info Spec	Bentley,Gena	4/7/2014	11	5	75,094.00	17,196.53	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00016080	STAFF ASSISTANT	Franklin,Carolyn	6/15/1976	12	8	100,225.00	22,951.53	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00016549	Emergency Operations&Info Spec	Paulus,Curice O	12/17/2018	11	5	75,094.00	17,196.53	1.00	Term	Local/Federal
BN0	21	3000	3100	F	00016861	Emergency Operations&Info Spec	Hill,Anthony Q	3/30/2020	11	3	70,818.00	16,217.32	1.00	Term	Local/Federal
BN0	21	3000	3100	F	00018125	Emergency Operations&Info Spec	Bowen-Thompson,CharMaine	1/22/2019	11	5	75,094.00	17,196.53	1.00	Term	Local/Federal
BN0	21	3000	3100	V	00019500	Emergency Operations&Info Spec			11	0	66,542.00	15,238.12	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00021430	Emergency Operations&Info Spec	Senhouse,Eustace M	3/17/2008	11	5	75,094.00	17,196.53	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00023961	Deputy Chief of Operations	Sneed Jr.,Robert W	3/19/2007	13	0	110,376.04	25,276.11	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00026092	Deputy Chief of Operations	Goldsmith,Frederick W.	3/3/2008	14	0	128,176.88	29,352.51	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00026503	Emergency Operations&Info Spec	McMahan,Alexander	8/22/2016	11	6	77,232.00	17,686.13	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00027054	Emergency Operations&Info Spec	Lewis III,Robert L.	3/10/2014	11	6	77,232.00	17,686.13	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00072950	Emergency Operations&Info Spec	Boone,William E	2/28/2011	9	10	71,106.00	16,283.27	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00073707	Plans & Preparedness Officer	Akasa,Annah	5/20/2013	14	10	133,537.00	30,579.97	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00075236	Supvy Emerg Oper & Info Spec.	Harris,Robert S	7/11/2005	12	0	94,554.00	21,652.87	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00075240	Deputy Chief of Operations	Scott II,Renaud D.	3/16/2020	14	0	129,411.00	29,635.12	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00088354	Emergency Operations&Info Spec	Stanton,Nyema	3/21/2016	11	7	79,370.00	18,175.73	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00088356	Emergency Operations&Info Spec	Armstrong,Tiffany N.	3/21/2016	11	5	75,094.00	17,196.53	1.00	Reg	Local/Federal
BN0	21	3000	3100	F	00091360	CHIEF OF OPERATIONS	Osborn,William	1/9/2017	16	0	170,000.00	38,930.00	1.00	Reg	Local/Federal
BN0	21	3000	3100	V	00095587	Chief of Staff			15	0	143,646.00	32,894.93	1.00	Reg	Local/Federal
BN0	21	3000	3111	F	00088525	Deputy Chief of Operations	Lucas,Donte O	8/12/2013	14	0	129,854.16	29,736.60	1.00	Reg	Local/Federal
BN0	21	3000	3111	F	00002939	Program Analyst	Mc Dermott,Nicole M	7/22/2019	11	10	79,314.00	18,162.91	1.00	Term	Federal
BN0	21	3000	3111	F	00019028	Emergency Planning Specialist	Farley,James J.	11/12/2019	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	3000	3111	V	00037366	Emergency Planning Specialist			11	0	66,542.00	15,238.12	1.00	Reg	Federal
BN0	21	3000	3111	F	00097267	Emergency Planning Specialist	Partridge,Nathanial Steven	9/16/2019	9	10	71,106.00	16,283.27	1.00	Term	Federal
BN0	21	3000	3113	F	00073611	Attorney Advisor	Black,Dion E	8/20/2018	14	7	145,645.00	33,352.71	1.00	Reg	Federal
BN0	21	3000	3113	F	00085184	Geographic Information Systems	Lescure,William	5/4/2015	13	5	107,022.00	24,508.04	1.00	Reg	Federal
BN0	21	3000	3363	F	00048775	Statewide Communications Inter	Guddemi,Charles	8/21/2017	14	10	144,439.00	33,076.53	1.00	Term	Federal
BN0	21	3000	3363	V	00092021	Program Coordinator (State)			14	0	103,657.00	23,737.45	1.00	Reg	Federal
BN0	21	3000	3402	F	00082823	Logistics Management Specialis	Hauser,Eric	7/6/1999	12	6	95,111.00	21,780.42	1.00	Reg	Local/Federal
BN0	21	3000	3402	F	00085594	Community Outreach Specialist	Gilmore,Edward James	1/2/2015	6	0	103,321.71	23,660.67	1.00	Reg	Local/Federal
BN0	21	3000	3402	F	00091072	Facility Management Specialist	Ross Jr.,Thomas A.	11/9/2020	12	1	82,326.00	18,852.65	1.00	Term	Local/Federal
BN0	21	3000	3402	F	00094954	Logistics Management Specialis	Rodgers Jr.,Billy F.	11/18/2013	12	1	82,326.00	18,852.65	1.00	Reg	Local/Federal
BN0	21	3000	3402	F	00075239	Supv Mgmt and Program Analyst	Woodall,Kenneth	8/25/2014	14	0	140,080.00	32,078.32	1.00	Reg	Federal
BN0	21	3000	3402	F	00085181	Logistics Management Specialis	Harris,Jason Burnell	2/11/2015	12	5	92,554.00	21,194.87	1.00	Reg	Federal
BN0	21	3000	3402	F	00095365	Logistics Management Specialis	Jones,Cynthia J	10/1/2018	12	1	82,326.00	18,852.65	1.00	Term	Federal
BN0	21	4000	4100	F	00045220	Grants Program Manager	Ross,Cembrye Alma	7/15/2013	12	10	105,339.00	24,122.63	1.00	Reg	Federal
BN0	21	4000	4100	F	00045237	Chief, Grants Division	Madden,Charles E.F.	4/27/2009	15	0	135,982.86	31,140.07	1.00	Reg	Federal
BN0	21	4000	4100	F	00045242	Grants Management Specialist	Naughton,Ingrid E	11/19/2012	12	10	105,339.00	24,122.63	1.00	Term	Federal
BN0	21	4000	4100	F	00045269	Grants Program Manager	Sumbeida,Muniru	7/8/2019	12	6	95,111.00	21,780.42	1.00	Term	Federal
BN0	21	4000	4100	F	00045279	Grants Management Officer	Reed,Tristan F	4/27/2009	14	0	129,410.75	29,635.06	1.00	Reg	Federal
BN0	21	4000	4100	F	00048762	Grants Program Manager	Coleman,Bettina R	7/19/2010	13	7	113,104.00	25,900.82	1.00	Reg	Federal
BN0	21	4000	4100	F	00048766	Grants Specialist	Cuyler,Siobhan Taneisha	3/29/2010	13	10	122,227.00	27,989.98	1.00	Term	Federal
BN0	21	4000	4100	F	00048769	Grants Program Manager	Cooper,Sherelle D	12/17/2012	12	10	105,339.00	24,122.63	1.00	Term	Federal
BN0	21	4000	4100	F	00048771	Grants Program Manager	Woodall,Rachel	8/7/2017	12	10	105,339.00	24,122.63	1.00	Term	Federal
BN0	21	4000	4100	F	00072956	Grants Program Manager	Mudambo,Mildred	7/8/2019	12	10	105,339.00	24,122.63	1.00	Term	Federal
BN0	21	4000	4100	V	00076859	Grants Management Specialist			12	0	82,326.00	18,852.65	1.00	Reg	Federal
BN0	21	4000	4100	V	00094683	Grants Management Specialist			12	0	82,326.00	18,852.65	1.00	Reg	Federal
BN0	21	4000	4101	F	00075238	Emergency Planning Officer	Gardner,Russell	2/11/1980	14	5	126,479.00	28,963.69	1.00	Reg	Local/Federal
BN0	21	4000	4124	F	00082821	AGENCY FISCAL OFFICER	Nitz,John	11/19/2012	16	10	190,773.00	43,687.02	1.00	Reg	Local/Federal
BN0	21	4000	4124	F	00086143	BUDGET OFFICER	Iwobi,Anthony	10/9/2001	14	9	140,849.00	32,254.42	1.00	Reg	Local/Federal
BN0	21	4000	4124	F	00087482	BUDGET ANALYST	Withrow,Andre	4/9/2000	11	7	79,373.00	18,176.42	1.00	Reg	Local/Federal
BN0	21	4000	4124	F	00087483	Accounts Payable Technician	Billings,Sharita	5/31/2016	8	3	53,407.00	12,230.20	1.00	Reg	Federal
BN0	21	4000	4305	F	00018601	Supervisory IT Specialist	Plavan,Timur	2/22/2016	14	0	120,000.00	27,480.00	1.00	Reg	Local/Federal
BN0	21	4000	4305	F	00088110	Information Technology Spec.	Feast,Taijuana	11/30/2015	12	5	92,554.00	21,194.87	1.00	Term	Federal
BN0	21	4000	4305	V	00091071	Information Technology Spec			13	0	94,858.00	21,722.48	1.00	Reg	Federal
BN0	21	4000	4305	F	00095150	Information Technology Spec.	El Baamrani,Hamid	9/4/2018	12	5	92,554.00	21,194.87	1.00	Term	Federal
BN0	21	4000	4305	F	00095151	Information Technology Spec.	Cherinet,Hirut A	5/12/2014	12	5	92,554.00	21,194.87	1.00	Term	Federal
BN0	21	4000	4305	F	00095152	Information Technology Special	Cook,Erin	10/1/2018	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	4000	4305	V	00097009	Director of Policy, Planning a			14	0	103,657.00	23,737.45	1.00	Reg	Federal
BN0	21	4000	4FA0	F	00028224	Assist Dir for Administration	Gill,Adriane	1/19/2010	15	0	149,350.00	34,201.15	1.00	Reg	Local/Federal
BN0	21	4000	4FA0	F	00077400	Program Analyst	Bowen,Whitney S	3/25/2013	13	8	107,380.00	24,590.02	1.00	Reg	Local/Federal
BN0	21	4000	4FA1	F	00004563	Program Analyst	Valentine,Amanda	4/15/2019	11	8	81,508.00	18,665.33	1.00	Term	Local/Federal
BN0	21	4000	4FA1	F	00007908	PGM ANALYST	Huggins,Briana	3/7/2016	13	3	100,940.00	23,115.26	1.00	Term	Local/Federal
BN0	21	4000	4FA1	F	00077771	Program Analyst	Patel,Dishma	4/15/2019	11	5	75,094.00	17,196.53	1.00	Term	Local/Federal
BN0	21	4000	4FA1	F	00086264	Program Analyst	Hill,Monica	6/29/2015	11	6	77,232.00	17,686.13	1.00	Reg	Local/Federal
BN0	21	4000	4FA2	F	00016885	Human Resources Specialist	Bailey,Leah R.	11/12/2019	12	5	85,570.00	19,595.53	1.00	Term	Local/Federal
BN0	21	4000	4FA2	F	00016991	Human Resources Specialist	Crawley,Lorien	6/30/2014	13	6	101,758.00	23,302.58	1.00	Reg	Local/Federal
BN0	21	4000	4FA2	F	00045254	Human Resources Specialist	Terry,Andre R	8/13/2012	14	6	120,257.00	27,538.85	1.00	Reg	Local/Federal
BN0	21	5000	5101	F	00077401	Supervisory Intelligence Analy	Tepper,Alexandria	6/12/2017	13	0	112,531.00	25,769.60	1.00	Reg	Federal
BN0	21	5000	5101	F	00082016	Information Collection (IC3) W	Kornreich,Kevin	2/21/2006	11	5	75,094.00	17,196.53	1.00	Reg	Federal
BN0	21	5000	5101	F	00092091	Information Collection (IC3) W	Dorsey,Nicholas	8/31/2020	11	4	72,956.00	16,706.92	1.00	Term	Federal
BN0	21	5000	5101	F	00092092	Information Collection (IC3) W	Rinonos,David	5/30/2017	11	6	77,232.00	17,686.13	1.00	Term	Federal
BN0	21	5000	5101	F	00092093	Information Collection (IC3) W	Hewitt,Megan	5/30/2017	11	6	77,232.00	17,686.13	1.00	Term	Federal
BN0	21	5000	5101	F	00092374	Information Collection (IC3) W	Washington,Amber D	8/20/2018	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	5000	5101	F	00092375	Information Collection (IC3) W	McCrimmon,Rhonda R	1/7/2019	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	5000	5101	F	00092376	Information Collection (IC3) W	Dean-Johnson,Kendra	2/4/2019	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	5000	5101	F	00095363	Information Collection (IC3) W	Freeman,Brittany	8/31/2020	11	4	72,956.00	16,706.92	1.00	Term	Federal
BN0	21	5000	5101	F	00095364	Information Collection (IC3) W	Evans,Tasha S.	8/20/2018	11	5	75,094.00	17,196.53	1.00	Term	Federal
BN0	21	5000	5132	F	00024310	Telecommunications Spec (COMSE	Curry,William W	11/13/1985	13	8	116,145.00	26,597.21	1.00	Reg	Local/Federal
BN0	21	5000	5132	F	00085114	Program Analyst	Miller,Sonia A	10/15/2018	12	6	95,111.00	21,780.42	1.00	Term	Federal
BN0	21	5000	5132	F	00094682	Plans and Preparedness Officer	Harvin,Dawn	8/12/2014	15	0	153,470.00	35,144.63	1.00	Reg	Federal
BN0	21	5000	5132	F	00097140	Program Coordinator	Mein,John M.	10/15/2012	14	9	130,217.00	29,819.69	1.00	Reg	Federal
BN0	21	5000	5133	V	00077541	Supervisory Intelligence Analy			14	0	129,411.00	29,635.12	1.00	Reg	Federal
BN0	21	5000	5182	V	00077539	Staff Assistant			12	0	76,126.00	17,432.85	1.00	Reg	Federal
BN0	21	5000	5182	F	00077728	Supervisory Intelligence Analy	Marcenelle,Madeline	5/30/2017	14	0	120,500.00	27,594.50	1.00	Reg	Federal
BN0	21	5000	5182	V	00077877	Fusion Intelligence Analyst			11	0	66,542.00	15,238.12	1.00	Reg	Federal
BN0	21	5000	5182	F	00077970	Supervisory Intelligence Analy	Bovia,Darrin M.	11/9/2020	13	0	120,000.00	27,480.00	1.00	Reg	Federal
BN0	21	5000	5182	F	00077971	Fusion Intelligence Analyst	Ferraro,Alexandra	4/27/2020	11	4	72,956.00	16,706.92	1.00	Term	Federal
BN0	21	5000	5182	V	00085111	Fusion Intelligence Analyst			13	0	94,858.00	21,722.48	1.00	Reg	Federal
BN0	21	5000	5182	F	00085112	Fusion Intelligence Analyst	Ross,Aaron	4/27/2020	12	4	89,997.00	20,609.31	1.00	Term	Federal
BN0	21	5000	5182	F	00085179	Fusion Intelligence Analyst	Lambert,Jordan J.	4/27/2020	12	4	89,997.00	20,609.31	1.00	Term	Federal
BN0	21	5000	5182	V	00085180	Fusion Intelligence Analyst			12	0	82,326.00	18,852.65	1.00	Reg	Federal
BN0	21	5000	5182	F	00085182	Fusion Intelligence Analyst	Hoodjer,Steven	12/17/2018	11	3	70,818.00	16,217.32	1.00	Term	Federal
BN0	21	5000	5182	F	00097013	Fusion Intelligence Analyst	Knight,Trevor Charles	4/27/2020	12	4	89,997.00	20,609.31	1.00	Term	Federal
BN0	21	5000	5182	V	00097263	Fusion Intelligence Analyst			9	0	55,230.00	12,647.67	1.00	Reg	Federal
BN0	21	5000	5182	F	00097265	Fusion Intelligence Analyst	Ehlman,Sarah E.	1/7/2019	11	1	66,542.00	15,238.12	1.00	Term	Federal
BN0	21	5000	5182	F	00097266	Fusion Intelligence Analyst	Spalding,Jordan	10/13/2020	11	4	72,956.00	16,706.92	1.00	Term	Federal
BN0	21	5000	5183	F	00047136	Fusion Intelligence Analyst	Randolph,Sedley A	1/21/2020	9	5	62,286.00	14,263.49	1.00	Term	Federal
BN0	21	5000	5183	F	00097014	Fusion Intelligence Analyst	Peri,David	12/17/2018	11	10	85,784.00	19,644.54	1.00	Term	Federal
BN0	21	5000	5183	V	00097262	Fusion Intelligence Analyst			13	0	94,858.00	21,722.48	1.00	Reg	Federal
AGENCY GRAND TOTAL											**$ 14,374,238.33**	**$ 3,291,700.60**	**142.00**		

Q4 HSEMA

Included below is a current vehicle and accident list as of February 03, 2021.

Please note the individuals listed may not have been the individuals driving on the accident date. Some vehicles have been re-assigned.

Vehicle	Tag	Acquisition	Assignment	Accident Date
Chevy Tahoe 2017	G62-0841U	Leased	Chris Rodriguez	None
Dodge Durango 2016	G62-0057S	Leased	City Administrator	6/5/2020
Ford Explorer 2014	G62-3599N	Leased	EOM	None
Chevy Tahoe 2018	G62 1664V	Leased	Clint Osborn	None
Chevy Tahoe 2018	G62 3993S	Leased	Renaud Scott	None
Dodge Durango 2014	G62-2532P	Leased	Donte Lucas	None
Dodge Durango 2020	G62-1607X	Leased	Robert Sneed	None
Dodge Durango 2016	G62-2285R	Leased	SLT Vehicle	None
Suburban 2016Chevy	G62-1294S	Leased	Operations	None
Chevy Tahoe 2019	G62-1851W	Leased	Operations	None
Chevy Suburban 2014	G62-1071N	Leased	Operations	None
Dodge Durango 2014	G62-0760P	Leased	Fleet	None
Ford Flex 2019	G61-1279W	Leased	Fleet	None
Ford Expedition 2014	G62-2542P	Leased	Fleet	None
Freightliner Columbia 2007	DC-8362	Owned	DC-12 MCC (Ops Division)	None
Kenworth T370 2019	DC-13238	Owned	DC-13 MCC (Ops Division)	None
Whisperwatt DCA-70SSJU 2004	603380	Owned	Generator	None
Whisperwatt DCA-70SSJU 2008	603541	Owned	Generator	None
DOOSAN 608950 6KW PORTABLE LIGHT TOWER 2016	DC-8950	Owned	Light Tower	None

DOOSAN 608949 6KW PORTABLE LIGHT TOWER 2016	DC-8949	Owned	Light Tower	None
Aisle Master 33NF 2019	45285	Owned	Logistics (yellow)	None
Uline 48x40 Forklift Aerial Platform 2020	H-2776	Owned	Logistics (yellow)	None
Yale A390 2019	DC-0000010973HS	Owned	Logistics (yellow)	None
Chevy Silverado 2018	G63-0971V	Leased	Logistics	4/20/20
Nexhaul Trailer 2020	22183	Owned	Utility Vehicles (white)	None
Utility Trailer CargoMate 2000	None	Owned	Utility Vehicles (white)	None
Pace America Utility Trailer OutBack 2000	DC-7968	Owned	Utility Vehicles (blue)	None
Pace America Utility Trailer Paceamerica 2000	DC-7241	Owned	Utility Vehicles (gray)	None

Q9 HSEMA

FY 2020

Transaction ID	Transaction Date	Post Date	Merchant Name	Debit Amount	Credit Amount	Purpose
Amanda Valentine *0477						
2962976666001	12/10/2019	12/11/2019	BLUE BOY PRINTING CORP	$370.00	$0.00	Professional Services
2969991441001	12/19/2019	12/20/2019	DELTA	$559.00	$0.00	Airline
2969991442001	12/19/2019	12/20/2019	VARIDESK* 1800 207 25	$405.00	$0.00	Supplies
2976572029001	01/06/2020	01/07/2020	MVS	$214.40	$0.00	Professional Services
2988628426001	01/22/2020	01/23/2020	INT*IN *SUPRETECH, INC	$152.26	$0.00	Computer, Hardware, Software and Peripherals
2990951678001	01/24/2020	01/27/2020	SLI DO	$1,200.00	$0.00	Computer, Hardware, Software and Peripherals
2993050129001	01/28/2020	01/29/2020	CALVIN PRICE GROUP	$1,205.02	$0.00	6
2995090844001	01/30/2020	01/31/2020	GEIGER - ECOMMERCE PLP	$647.99	$0.00	Supplies
2997525928001	02/03/2020	02/04/2020	SMK	$954.00	$0.00	Professional Services
2999451054001	02/05/2020	02/06/2020	CUA PARKING	$175.00	$0.00	Education
3009968541001	02/19/2020	02/20/2020	ATLANTA	$295.00	$0.00	Professional Services
3009968542001	02/19/2020	02/20/2020	GEORGE MASON UNIV MKTP	$550.00	$0.00	Education
3009968543001	02/19/2020	02/20/2020	ANNIES ACE HARDWARE	$419.99	$0.00	Supplies
3010989246001	02/19/2020	02/21/2020	SOUTHWEST	$628.96	$0.00	Airline
3010989247001	02/20/2020	02/21/2020	SKILLPATH / NATIONAL	$149.00	$0.00	Education
3010989248001	02/19/2020	02/21/2020	DELTA	$299.80	$0.00	Airline
3012276765001	02/21/2020	02/24/2020	ATLANTA	$295.00	$0.00	Professional Services
3012276766001	02/21/2020	02/24/2020	ASSOC FOR TALENT DEV	$245.00	$0.00	Professional Services
3012276767001	02/21/2020	02/24/2020	SOUTHWEST	$279.96	$0.00	Airline
3014390343001	02/25/2020	02/26/2020	ACCUWEATHER INC	$199.95	$0.00	Media and Advertising Services
3014390344001	02/25/2020	02/26/2020	BLUEBAY OFFICE INC	$861.83	$0.00	Supplies
3015404416001	02/26/2020	02/27/2020	NATIONAL EMERGENCY TRA	$71.28	$0.00	Restaurants
3031568946001	03/26/2020	03/27/2020	THE HAMILTON GROUP	$2,825.00	$0.00	Supplies
3032041459001	03/26/2020	03/30/2020	JIMMIE MUSCATELO'S WASHINGTON UNIFORM CENTER	$2,577.96	$0.00	Supplies
3034098705001	04/03/2020	04/06/2020	SCREENFLEX PORTABLE PA	$2,875.77	$0.00	Supplies
3041436325001	04/30/2020	05/01/2020	SOUTHWEST	$0.00	-$279.96	Airline
3047573855001	05/19/2020	05/20/2020	ATLANTA	$0.00	-$295.00	Professional Services
3047573856001	05/19/2020	05/20/2020	ATLANTA	$0.00	-$295.00	Professional Services
3053558931001	06/04/2020	06/05/2020	THE HAMILTON GROUP	$60.25	$0.00	Supplies
3054230334001	06/05/2020	06/08/2020	MAMA'S PIZZA	$120.00	$0.00	Restaurants
3057177042001	06/12/2020	06/15/2020	SENODA INC	$1,881.00	$0.00	Professional Services
3060974778001	06/23/2020	06/23/2020	ULINE	$907.44	$0.00	Supplies
3062544199001	06/25/2020	06/26/2020	GRAINGER	$1,391.92	$0.00	Supplies
3063272565001	06/26/2020	06/29/2020	EVERBRIDGE INC	$1,000.00	$0.00	Computer, Hardware, Software and Peripherals
3064068496001	06/29/2020	06/30/2020	THE HAMILTON GROUP	$1,693.23	$0.00	Supplies
3074167467001	07/22/2020	07/23/2020	GEIGER - ECOMMERCE PLP	$490.20	$0.00	Supplies
3077368513001	07/29/2020	07/30/2020	EVERBRIDGE INC	$188.58	$0.00	Computer, Hardware, Software and Peripherals
3081256882001	08/06/2020	08/07/2020	METRO WASHINGTON COUNC	$1,000.00	$0.00	Computer, Hardware, Software and Peripherals
3082939309001	08/10/2020	08/11/2020	METROPOLITAN OFFICE PR	$3,162.52	$0.00	Computer, Hardware, Software and Peripherals
3083787394001	08/11/2020	08/12/2020	METROPOLITAN OFFICE PR	$94.23	$0.00	Computer, Hardware, Software and Peripherals
3084370775001	08/12/2020	08/13/2020	SMK	$384.00	$0.00	Professional Services
3087876249001	08/19/2020	08/20/2020	MOBIL SATELLITE TECHNO	$1,950.15	$0.00	Utilities
3093677817001	08/31/2020	09/01/2020	STK*SHUTTERSTOCK	$2,028.00	$0.00	Professional Services
3097452359001	09/08/2020	09/09/2020	METROPOLITAN OFFICE PR	$975.00	$0.00	Computer, Hardware, Software and Peripherals
3097452360001	09/08/2020	09/09/2020	METROPOLITAN OFFICE PR	$1,622.17	$0.00	Computer, Hardware, Software and Peripherals

3098629346001	09/10/2020	09/11/2020	IN *SUPRETECH, INC.	$4,874.72	$0.00	Professional Services
3100327227001	09/14/2020	09/15/2020	THE HAMILTON GROUP	$3,159.00	$0.00	Supplies
3100917109001	09/15/2020	09/16/2020	SQ *PTS, INC.	$2,744.00	$0.00	Professional Services
3100917110001	09/15/2020	09/16/2020	HOO*HOOTSUITE INC	$1,188.00	$0.00	Professional Services
3101526808001	09/16/2020	09/17/2020	HOO*HOOTSUITE INC	$1,188.00	$0.00	Professional Services
3101526809001	09/16/2020	09/17/2020	MVS INC	$2,019.41	$0.00	Professional Services
Dishma Patel *7063						
2918759089001	10/10/2019	10/11/2019	NAT FUSION CTR ASSN	$375.00	$0.00	Education
2918759090001	10/10/2019	10/11/2019	NAT FUSION CTR ASSN	$375.00	$0.00	Education
2920319474001	10/11/2019	10/14/2019	LEXISNEXIS RISK SOL EP	$300.00	$0.00	Professional Services
2920319475001	10/11/2019	10/14/2019	LEXISNEXIS RISK SOL EP	$300.00	$0.00	Professional Services
2920319476001	10/11/2019	10/14/2019	LEXISNEXIS RISK SOL EP	$300.00	$0.00	Professional Services
2921126784001	10/15/2019	10/15/2019	SMARTSIGN	$1,258.69	$0.00	Professional Services
2922056353001	10/15/2019	10/16/2019	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
2925681787001	10/18/2019	10/21/2019	UNITED AIRLINES	$1,234.60	$0.00	Airline
2925681788001	10/18/2019	10/21/2019	UNITED AIRLINES	$1,234.60	$0.00	Airline
2925681789001	10/18/2019	10/21/2019	UNITED AIRLINES	$1,234.60	$0.00	Airline
2925681790001	10/18/2019	10/21/2019	AMERICAN AIRLINES	$1,250.50	$0.00	Airline
2935184870001	10/30/2019	11/01/2019	AMERICAN AIRLINES	$361.30	$0.00	Airline
2935184871001	10/30/2019	11/01/2019	AMERICAN AIRLINES	$67.95	$0.00	Airline
2935184872001	10/31/2019	11/01/2019	SKILLPATH / NATIONAL	$798.00	$0.00	Education
2935184873001	10/31/2019	11/01/2019	WRLD OF FORD SALES INC	$439.90	$0.00	Vehicle Maintenance and Fuel Services
2937479031001	11/04/2019	11/05/2019	PAYPAL	$650.00	$0.00	Professional Services
2938423303001	11/05/2019	11/06/2019	INT*IN *SUPRETECH, INC	$380.90	$0.00	Professional Services
2938423304001	11/05/2019	11/06/2019	CALIFORNIA SOCIETY OF	$585.00	$0.00	Professional Services
2939447274001	11/06/2019	11/07/2019	INTERNATIONAL ASSOCIAT	$842.00	$0.00	Education
2941742048001	11/08/2019	11/11/2019	WIX*WIX.COM, INC.	$324.00	$0.00	Computer, Hardware, Software and Peripherals
2943740324001	11/12/2019	11/13/2019	INTERNATIONAL ASSOCIAT	$195.00	$0.00	Education
2943740325001	11/12/2019	11/13/2019	INTERNATIONAL ASSOCIAT	$726.00	$0.00	Education
2943740326001	11/12/2019	11/13/2019	DSS CORPORATION	$5,000.00	$0.00	Professional Services
2944759281001	11/12/2019	11/14/2019	AMERICAN AIRLINES	$794.60	$0.00	Airline
2945796911001	11/15/2019	11/15/2019	ULINE	$442.62	$0.00	Professional Services
2945796912001	11/13/2019	11/15/2019	AMTRAK .CO31	$102.00	$0.00	Transportation
2945796913001	11/14/2019	11/15/2019	US AIR PURIFIERS LLC	$999.00	$0.00	Supplies
2945796914001	11/14/2019	11/15/2019	METROPOLITAN OFFICE PR	$206.54	$0.00	Computer, Hardware, Software and Peripherals
2947077606001	11/15/2019	11/18/2019	AMZN MKTP US	$295.99	$0.00	Supplies
2947077607001	11/14/2019	11/18/2019	CCBC	$561.00	$0.00	Education
2947077608001	11/15/2019	11/18/2019	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
2947077609001	11/15/2019	11/18/2019	CALIFORNIA SOCIETY OF	$585.00	$0.00	Professional Services
2947077610001	11/15/2019	11/18/2019	AMTRAK .CO31	$169.00	$0.00	Transportation
2948239627001	11/18/2019	11/19/2019	CHAMPION AWARDS	$125.00	$0.00	Supplies
2950193334001	11/20/2019	11/21/2019	WASP BAR CODE	$1,985.07	$0.00	Supplies
2950193335001	11/12/2019	11/21/2019	CAPITAL SERVICES & SUP	$1,995.93	$0.00	Supplies
2950193336001	11/14/2019	11/21/2019	CAPITAL SERVICES & SUP	$644.85	$0.00	Supplies
2951207205001	11/21/2019	11/22/2019	DTV	$222.98	$0.00	Utilities
2951207206001	11/21/2019	11/22/2019	FEDEX	$5.21	$0.00	Professional Services
2952429778001	11/21/2019	11/25/2019	LEXISNEXIS RISK SOL EP	$300.00	$0.00	Professional Services
2952429779001	11/23/2019	11/25/2019	WIX.COM	$14.95	$0.00	Professional Services

2956521620001	12/02/2019	12/03/2019	PIPPA PODCAST SERVICES	$240.00	$0.00	Computer, Hardware, Software and Peripherals
2957469052001	12/03/2019	12/04/2019	TEEM TECHNOLOGIES	$1,000.00	$0.00	Computer, Hardware, Software and Peripherals
2958489310001	12/05/2019	12/05/2019	ULINE	$562.23	$0.00	Professional Services
2959524017001	12/05/2019	12/06/2019	DTV	$227.23	$0.00	Utilities
2959524018001	12/04/2019	12/06/2019	LEXISNEXIS RISK SOL EP	$300.00	$0.00	Professional Services
2962030531001	12/09/2019	12/10/2019	INT*IN *SUPRETECH, INC	$1,787.18	$0.00	Professional Services
2962030532001	12/09/2019	12/10/2019	CALIFORNIA SOCIETY OF	$75.00	$0.00	Professional Services
2962976751001	12/10/2019	12/11/2019	NATIONAL EMERGENCY TRA	$71.28	$0.00	Restaurants
2966263102001	12/12/2019	12/16/2019	UNITED AIRLINES	$547.00	$0.00	Airline
2966263103001	12/12/2019	12/16/2019	AMERICAN AIRLINES	$149.30	$0.00	Airline
2966263104001	12/12/2019	12/16/2019	AMERICAN AIRLINES	$494.30	$0.00	Airline
2966263105001	12/13/2019	12/16/2019	EVENTSDC	$900.00	$0.00	Professional Services
2966263106001	12/13/2019	12/16/2019	AMERICAN AIRLINES	$886.21	$0.00	Airline
2966263107001	12/13/2019	12/16/2019	AMERICAN AIRLINES	$149.30	$0.00	Airline
2966263108001	12/13/2019	12/16/2019	AMERICAN AIRLINES	$55.02	$0.00	Airline
2966263109001	12/13/2019	12/16/2019	AMERICAN AIRLINES	$25.00	$0.00	Airline
2966263110001	12/13/2019	12/16/2019	AMERICAN AIRLINES	$25.00	$0.00	Airline
2966263111001	12/15/2019	12/16/2019	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
2968193017001	12/17/2019	12/18/2019	SQU*SQ *ENVIRONMENTAL	$300.00	$0.00	Professional Services
2968193018001	12/17/2019	12/18/2019	LOCKMASTERS INC	$2,700.00	$0.00	Professional Services
2968193019001	12/17/2019	12/18/2019	THE HAMILTON GROUP	$2,310.00	$0.00	Supplies
2969097128001	12/18/2019	12/19/2019	SAFELITE ONLINE PAYMEN	$99.97	$0.00	Vehicle Maintenance and Fuel Services
2972164332001	12/23/2019	12/26/2019	AQUATOMIC PRODUCTS CO.	$450.00	$0.00	Supplies
2972164333001	12/24/2019	12/26/2019	AMERICAN AIRLINES	$0.00	-$36.54	Airline
2973075561001	12/27/2019	12/30/2019	DTV	$222.98	$0.00	Utilities
2975623962001	01/03/2020	01/06/2020	GEORGE MASON UNIVERSIT	$996.00	$0.00	Education
2977424636001	01/06/2020	01/08/2020	AMERICAN AIRLINES	$948.56	$0.00	Airline
2977424637001	01/06/2020	01/08/2020	AMERICAN AIRLINES	$25.00	$0.00	Airline
2978358911001	01/07/2020	01/09/2020	AMERICAN AIRLINES	$298.60	$0.00	Airline
2978358912001	01/07/2020	01/09/2020	ALASKA A 02	$297.80	$0.00	Airline
2979308326001	01/08/2020	01/10/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
2980527234001	01/09/2020	01/13/2020	AMERICAN AIRLINES	$669.80	$0.00	Airline
2981665349001	01/14/2020	01/14/2020	AMERICAN AIRLINES	$0.00	-$55.02	Airline
2984602721001	01/17/2020	01/17/2020	AMERICAN AIRLINES	$0.00	-$18.48	Airline
2984602722001	01/17/2020	01/17/2020	AMERICAN AIRLINES	$55.02	$0.00	Airline
2988628518001	01/23/2020	01/23/2020	APPLE.COM/US	$104.94	$0.00	Computer, Hardware, Software and Peripherals
2988628519001	01/22/2020	01/23/2020	US AIR PURIFIERS LLC	$2,409.00	$0.00	Supplies
2989658503001	01/24/2020	01/24/2020	APPLE.COM/US	$0.00	-$5.94	Computer, Hardware, Software and Peripherals
2989658504001	01/22/2020	01/24/2020	AMERICAN AIRLINES	$944.90	$0.00	Airline
2990951831001	01/24/2020	01/27/2020	VARIDESK* 1800 207 25	$1,620.00	$0.00	Supplies
3000471677001	02/06/2020	02/07/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3001769064001	02/07/2020	02/10/2020	BALDWIN GRAPHICS	$964.81	$0.00	Professional Services
3001769065001	02/07/2020	02/10/2020	DUTCH MILL CATERING LL	$4,995.75	$0.00	Restaurants
3002955197001	02/10/2020	02/11/2020	THOMSON REUTERS LEGAL	$403.00	$0.00	Professional Services
3005956515001	02/12/2020	02/14/2020	STANDARD OFFICE SUPPLY	$4,968.05	$0.00	Supplies
3007155724001	02/15/2020	02/17/2020	SPROUT SOCIAL, INC	$263.94	$0.00	Computer, Hardware, Software and Peripherals
3014390485001	02/24/2020	02/26/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3015404508001	02/26/2020	02/27/2020	NACCHO	$735.00	$0.00	Education

3016431402001	02/27/2020	02/28/2020	EFORENSICSMAG.COM	$450.00	$0.00	Computer, Hardware, Software and Peripherals
3016431403001	02/26/2020	02/28/2020	SOUTHWEST	$315.97	$0.00	Airline
3020686206001	03/04/2020	03/05/2020	ATLASSIAN	$3,500.00	$0.00	Computer, Hardware, Software and Peripherals
3020686207001	03/04/2020	03/05/2020	DTV	$229.99	$0.00	Utilities
3025421091001	03/11/2020	03/12/2020	ANNIES ACE HARDWARE	$36.98	$0.00	Supplies
3027126520001	03/15/2020	03/16/2020	SPROUT SOCIAL, INC	$263.94	$0.00	Computer, Hardware, Software and Peripherals
3028343571001	03/17/2020	03/18/2020	THE HAMILTON GROUP	$350.00	$0.00	Supplies
3028815057001	03/18/2020	03/19/2020	LEDO PIZZA H-ST	$217.69	$0.00	Restaurants
3029293718001	03/19/2020	03/20/2020	BLUEBAY OFFICE INC	$3,994.00	$0.00	Supplies
3032041503001	03/27/2020	03/30/2020	METROPOLITAN OFFICE PR	$1,084.93	$0.00	Computer, Hardware, Software and Peripherals
3034552618001	04/06/2020	04/07/2020	SPROUT SOCIAL, INC	$0.00	-$29.88	Computer, Hardware, Software and Peripherals
3035597351001	04/09/2020	04/10/2020	DTV	$229.99	$0.00	Utilities
3035597352001	04/09/2020	04/10/2020	IN *BRIAR PATCH SHREDD	$203.00	$0.00	Professional Services
3035597353001	04/08/2020	04/10/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3035597354001	04/08/2020	04/10/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3037063180001	04/15/2020	04/16/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3038288951001	04/20/2020	04/21/2020	FEEDLY.COM	$192.00	$0.00	Professional Services
3038987151001	04/22/2020	04/23/2020	NACCHO	$0.00	-$735.00	Education
3041046146001	04/29/2020	04/30/2020	IN *SUPRETECH, INC.	$1,994.00	$0.00	Professional Services
3045594550001	05/13/2020	05/14/2020	DTV	$229.99	$0.00	Utilities
3046012468001	05/14/2020	05/15/2020	THOMSON REUTERS LEGAL	$302.25	$0.00	Professional Services
3046567768001	05/15/2020	05/18/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3048009555001	05/20/2020	05/21/2020	WIX.COM	$623.28	$0.00	Professional Services
3049855809001	05/26/2020	05/27/2020	PAPA JOHN'S #3540	$466.94	$0.00	Restaurants
3051405278001	05/30/2020	06/01/2020	WIX.COM	$126.94	$0.00	Professional Services
3053065274001	06/03/2020	06/04/2020	MAMA'S PIZZA	$120.00	$0.00	Restaurants
3053065275001	06/02/2020	06/04/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3053558962001	06/04/2020	06/05/2020	WIX.COM	$0.00	-$35.28	Professional Services
3053558963001	06/04/2020	06/05/2020	WIX.COM	$0.00	-$7.18	Professional Services
3056472744001	06/11/2020	06/12/2020	THOMSON REUTERS LEGAL	$1,400.00	$0.00	Professional Services
3057177091001	06/11/2020	06/15/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3057942350001	06/15/2020	06/16/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3061493614001	06/22/2020	06/24/2020	FEEDLY.COM	$0.00	-$192.00	Professional Services
3062016947001	06/24/2020	06/25/2020	DTV	$464.23	$0.00	Utilities
3067903149001	07/08/2020	07/09/2020	IN *INFRAGARD NATIONAL	$2,205.00	$0.00	Professional Services
3071007025001	07/15/2020	07/16/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3072281853001	07/19/2020	07/20/2020	FEEDLY.COM	$1,080.00	$0.00	Professional Services
3080121929001	08/04/2020	08/05/2020	FEWER CARDS	$799.60	$0.00	Supplies
3080682198001	08/05/2020	08/06/2020	METROPOLITAN OFFICE PR	$1,999.50	$0.00	Computer, Hardware, Software and Peripherals
3082022253001	08/07/2020	08/10/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3082022254001	08/07/2020	08/10/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3085765139001	08/15/2020	08/17/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals
3087276469001	08/18/2020	08/19/2020	DTV	$694.22	$0.00	Utilities
3094273185001	09/01/2020	09/02/2020	IN *BRIAR PATCH SHREDD	$588.00	$0.00	Professional Services
3094885631001	09/02/2020	09/03/2020	OTTER.AI	$99.99	$0.00	Professional Services
3098629408001	09/09/2020	09/11/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3099442377001	09/11/2020	09/14/2020	SQ *ZEKE'S COFFEE OF D	$2,266.00	$0.00	Restaurants
3100917185001	09/15/2020	09/16/2020	SPROUT SOCIAL, INC	$249.00	$0.00	Computer, Hardware, Software and Peripherals

3105753596001	09/24/2020	09/25/2020	AOP BUSINESS SERVICES	$364.84	$0.00	Supplies
Donte Lucas *5407						
3072281816001	07/17/2020	07/20/2020	LEDO PIZZA H-ST OL	$354.85	$0.00	Restaurants
Elijah Crawford *5039						
2922056349001	10/15/2019	10/16/2019	WPY	$895.00	$0.00	Professional Services
2929554314001	10/23/2019	10/25/2019	UNITED AIRLINES	$546.60	$0.00	Airline
2963996352001	12/11/2019	12/12/2019	INT*IN *AWARDS AND MOR	$4,000.00	$0.00	Supplies
2977424607001	01/07/2020	01/08/2020	ALTON MEMORIAL HEALTH	$0.01	$0.00	Professional Services
2985850561001	01/18/2020	01/20/2020	FRAUD CREDIT	$0.00	-$0.01	Transaction Dispute
2993050328001	01/28/2020	01/29/2020	STAPLES DIRECT	$634.33	$0.00	Supplies
2996367121001	02/01/2020	02/03/2020	ADMIN PROF CONFERENCE	$1,900.00	$0.00	Professional Services
3015404572001	02/26/2020	02/27/2020	CSG NEMA CC	$550.00	$0.00	Education
3015404573001	02/26/2020	02/27/2020	CSG NEMA CC	$550.00	$0.00	Education
3015404574001	02/26/2020	02/27/2020	CSG NEMA CC	$550.00	$0.00	Education
3015404575001	02/26/2020	02/27/2020	CSG NEMA CC	$550.00	$0.00	Education
3015404576001	02/26/2020	02/27/2020	CSG NEMA CC	$550.00	$0.00	Education
3017706869001	02/28/2020	03/02/2020	UNITED AIRLINES	$780.80	$0.00	Airline
3023838263001	03/09/2020	03/10/2020	NEW YORK TIMES DIGITAL	$8.48	$0.00	Professional Services
3023838264001	03/09/2020	03/10/2020	SUB	$30.74	$0.00	Professional Services
3024604723001	03/11/2020	03/11/2020	D J	$20.66	$0.00	Professional Services
3028815090001	03/18/2020	03/19/2020	GIANT 2376	$70.43	$0.00	Supplies
3028815091001	03/17/2020	03/19/2020	CSG NEMA CC	$0.00	-$550.00	Education
3028815092001	03/17/2020	03/19/2020	CSG NEMA CC	$0.00	-$550.00	Education
3028815093001	03/17/2020	03/19/2020	CSG NEMA CC	$0.00	-$550.00	Education
3028815094001	03/17/2020	03/19/2020	CSG NEMA CC	$0.00	-$550.00	Education
3028815095001	03/17/2020	03/19/2020	CSG NEMA CC	$0.00	-$550.00	Education
3034098792001	04/04/2020	04/06/2020	NEW YORK B CNTR PORT AUTH	$8.48	$0.00	Professional Services
3035597373001	04/10/2020	04/10/2020	D J	$20.66	$0.00	Professional Services
3041965953001	05/02/2020	05/04/2020	NEW YORK B CNTR PORT AUTH	$8.48	$0.00	Professional Services
3044236297001	05/10/2020	05/11/2020	D J	$20.66	$0.00	Professional Services
3051405314001	05/30/2020	06/01/2020	NYTIMES	$8.48	$0.00	Professional Services
3055453618001	06/10/2020	06/10/2020	D J	$20.66	$0.00	Professional Services
3063272651001	06/27/2020	06/29/2020	NYTIMES	$8.48	$0.00	Professional Services
3068430989001	07/10/2020	07/10/2020	D J	$20.66	$0.00	Professional Services
3069155176001	07/10/2020	07/13/2020	CSG NEMA CC	$4,500.00	$0.00	Education
3075461936001	07/25/2020	07/27/2020	NYTIMES	$8.48	$0.00	Professional Services
3082022288001	08/10/2020	08/10/2020	D J	$20.66	$0.00	Professional Services
3089318720001	08/22/2020	08/24/2020	NYTIMES	$8.48	$0.00	Professional Services
3098025183001	09/10/2020	09/10/2020	D J	$20.66	$0.00	Professional Services
3100327314001	09/14/2020	09/15/2020	THE HAMILTON GROUP	$45.95	$0.00	Supplies
3102985466001	09/19/2020	09/21/2020	NYTIMES	$8.48	$0.00	Professional Services
Monica Hill *1836						
2912760635001	10/02/2019	10/03/2019	DIGICERT INC	$412.00	$0.00	Professional Services
2925681771001	10/18/2019	10/21/2019	UNITED AIRLINES	$1,234.60	$0.00	Airline
2925681772001	10/18/2019	10/21/2019	UNITED AIRLINES	$1,234.60	$0.00	Airline
2925681773001	10/18/2019	10/21/2019	UNITED AIRLINES	$33.00	$0.00	Airline
2932069777001	10/28/2019	10/29/2019	INTERNATIONAL ASSOCIAT	$726.00	$0.00	Education
2933281422001	10/28/2019	10/30/2019	AMERICAN AIRLINES	$405.60	$0.00	Airline

2933281423001	10/28/2019	10/30/2019	AMERICAN AIRLINES	$48.32	$0.00	Airline
2948239617001	11/18/2019	11/19/2019	BLUEBAY OFFICE INC	$365.50	$0.00	Supplies
2952429736001	11/23/2019	11/25/2019	NATIONAL EMERGENCY TRA	$347.78	$0.00	Restaurants
2954146314001	11/26/2019	11/27/2019	INT*IN *SUPRETECH, INC	$1,101.90	$0.00	Professional Services
2954916709001	11/27/2019	11/29/2019	AMTRAK .CO33	$124.00	$0.00	Transportation
2954916710001	11/27/2019	11/29/2019	AMTRAK .CO33	$155.00	$0.00	Transportation
2957469043001	12/02/2019	12/04/2019	AMTRAK 33	$0.00	-$37.00	Transportation
2958489284001	12/04/2019	12/05/2019	NATIONAL EMERGENCY TRA	$0.00	-$20.47	Restaurants
2963996363001	12/11/2019	12/12/2019	NBA OFFICE PRODUCTS, I	$813.05	$0.00	Supplies
2965020070001	12/12/2019	12/13/2019	NBA OFFICE PRODUCTS, I	$20.60	$0.00	Supplies
2968193000001	12/17/2019	12/18/2019	DUTCH MILL CATERING LL	$987.50	$0.00	Restaurants
2990951805001	01/24/2020	01/27/2020	EVENTSDC	$900.00	$0.00	Professional Services
2995090917001	01/30/2020	01/31/2020	DTV	$222.98	$0.00	Utilities
3000471663001	02/06/2020	02/07/2020	SP * POWERBX	$1,822.54	$0.00	Computer, Hardware, Software and Peripherals
3002955192001	02/10/2020	02/11/2020	SP * POWERBX	$3,031.81	$0.00	Computer, Hardware, Software and Peripherals
3009968630001	02/19/2020	02/20/2020	IN *SUPRETECH, INC.	$527.80	$0.00	Professional Services
3010989336001	02/20/2020	02/21/2020	CAPITOL DOCUMENT SOLUTIONS, LLC	$245.80	$0.00	Professional Services
3018860165001	03/02/2020	03/03/2020	IN *SUPRETECH, INC.	$4,632.80	$0.00	Professional Services
3018860166001	03/02/2020	03/03/2020	IN *SUPRETECH, INC.	$314.54	$0.00	Professional Services
3019733095001	03/03/2020	03/04/2020	CALVIN PRICE GROUP	$1,608.43	$0.00	Professional Services
3020686185001	03/04/2020	03/05/2020	SMARTSIGN	$1,258.69	$0.00	Professional Services
3025421081001	03/11/2020	03/12/2020	AMERICAN BUSINESS SUPP	$4,459.73	$0.00	Professional Services
3033634037001	04/02/2020	04/03/2020	TEEM TECHNOLOGIES	$2,227.50	$0.00	Computer, Hardware, Software and Peripherals
3037851990001	04/17/2020	04/20/2020	AMERICAN BUSINESS SUPP	$159.98	$0.00	Professional Services
3049855800001	05/26/2020	05/27/2020	IN *SUPRETECH, INC.	$1,860.00	$0.00	Professional Services
3054961383001	06/05/2020	06/09/2020	CCBC	$1,053.00	$0.00	Education
3065110996001	07/02/2020	07/02/2020	WALLACE GROUP OF NY IN	$1,450.00	$0.00	Computer, Hardware, Software and Peripherals
3065110997001	07/01/2020	07/02/2020	IN *SUPRETECH, INC.	$1,393.00	$0.00	Professional Services
3065110998001	07/01/2020	07/02/2020	IN *SUPRETECH, INC.	$2,193.28	$0.00	Professional Services
3092801857001	08/28/2020	08/31/2020	MONA ELECTRIC GROUP IN	$1,590.00	$0.00	Professional Services
3102985305001	09/18/2020	09/21/2020	QUALTRICS	$381.60	$0.00	Computer, Hardware, Software and Peripherals
3102985306001	09/18/2020	09/21/2020	BLUEBAY OFFICE INC	$3,038.76	$0.00	Supplies
3102985307001	09/18/2020	09/21/2020	BLUEBAY OFFICE INC	$2,153.77	$0.00	Supplies
3104501723001	09/22/2020	09/23/2020	METROPOLITAN OFFICE PR	$3,279.95	$0.00	Computer, Hardware, Software and Peripherals
3106596274001	09/25/2020	09/28/2020	IN *SUPRETECH, INC.	$2,094.69	$0.00	Professional Services
Steven Benefield *2998						
2932069819001	10/28/2019	10/29/2019	FIRESTONE351414	$586.32	$0.00	Vehicle Maintenance and Fuel Services
2951207299001	11/21/2019	11/22/2019	MLK DELI	$1,435.00	$0.00	Restaurants

FY 2021

Transaction ID	Transaction Date	Post Date	Merchant Name	Debit Amount	Credit Amount	Purpose
Amanda Valentine *0477						
3123110598001	10/27/2020	10/28/2020	GEIGER - ECOMMERCE PLP	$1,449.97	$0.00	Professional Services
3123110599001	10/27/2020	10/28/2020	GEIGER - ECOMMERCE PLP	$1,799.49	$0.00	Professional Services
3123743203001	10/29/2020	10/29/2020	DISPUTE CREDIT	$0.00	-$1,188.00	Professional Services
3124375825001	10/29/2020	10/30/2020	GEIGER - MOTO IPT	$1,639.64	$0.00	Supplies
3124375826001	10/29/2020	10/30/2020	GEIGER - MOTO IPT	$0.00	-$1,449.97	Supplies
3125249424001	10/29/2020	11/02/2020	FASTSIGNS OF DC	$462.63	$0.00	Professional Services

3140819910001	12/01/2020	12/02/2020	METROPOLITAN OFFICE PR	$782.87	$0.00	Computer, Hardware, Software and Peripherals
3142974268001	12/06/2020	12/07/2020	KAPWING PRO PLAN	$20.00	$0.00	Computer, Hardware, Software and Peripherals
3146708649001	12/11/2020	12/14/2020	MLK DELI	$1,670.00	$0.00	Restaurants
3148908991001	12/16/2020	12/17/2020	SLI DO	$1,200.00	$0.00	Computer, Hardware, Software and Peripherals
3149528770001	12/17/2020	12/18/2020	SQ *ZEKE'S COFFEE OF D	$360.00	$0.00	Restaurants
3153712779001	12/28/2020	12/29/2020	IN *SUPRETECH, INC.	$764.49	$0.00	Professional Services
3153712780001	12/28/2020	12/29/2020	IN *BRIAR PATCH SHREDD	$265.00	$0.00	Professional Services
3154195766001	12/29/2020	12/30/2020	CALVIN PRICE GROUP	$527.92	$0.00	Professional Services
3154195767001	12/29/2020	12/30/2020	CALVIN PRICE GROUP	$1,199.96	$0.00	Professional Services
3154681167001	12/31/2020	12/31/2020	GIH*GLOBALINDUSTRIALEQ	$1,036.00	$0.00	Supplies
3157451029001	01/06/2021	01/07/2021	KAPWING PRO PLAN	$20.00	$0.00	Computer, Hardware, Software and Peripherals
3158858654001	01/08/2021	01/11/2021	PAYPAL	$2,720.00	$0.00	Supplies
3158858655001	01/08/2021	01/11/2021	CAPITAL SERVICES AND S	$127.90	$0.00	Professional Services
3158858656001	01/08/2021	01/11/2021	METROPOLITAN OFFICE PR	$1,346.48	$0.00	Computer, Hardware, Software and Peripherals
3158858657001	01/09/2021	01/11/2021	CALVIN PRICE GROUP	$189.83	$0.00	Professional Services
3160962767001	01/13/2021	01/14/2021	BLUEBAY OFFICE INC	$157.80	$0.00	Supplies
3163327049001	01/18/2021	01/19/2021	BLUEBAY OFFICE INC	$1,056.00	$0.00	Supplies
3164473293001	01/19/2021	01/21/2021	TRACTOR SUPPLY CO #550	$182.60	$0.00	Vehicle Maintenance and Fuel Services
3166863121001	01/25/2021	01/26/2021	ANNIES ACE HARDWARE	$286.00	$0.00	Supplies
3167445311001	01/26/2021	01/27/2021	AMZN MKTP US	$549.89	$0.00	Supplies
3167445312001	01/26/2021	01/27/2021	METROPOLITAN OFFICE PR	$236.49	$0.00	Computer, Hardware, Software and Peripherals
3167445313001	01/26/2021	01/27/2021	METROPOLITAN OFFICE PR	$78.58	$0.00	Computer, Hardware, Software and Peripherals
3167445314001	01/26/2021	01/27/2021	THE HAMILTON GROUP	$702.00	$0.00	Supplies
Dishma Patel *7063						
3109359073001	10/01/2020	10/02/2020	FEEDERCO	$4,160.00	$0.00	Computer, Hardware, Software and Peripherals
3109359074001	10/02/2020	10/02/2020	READYREFRESH BY NESTLE	$4,491.60	$0.00	Restaurants
3111766535001	10/06/2020	10/07/2020	DIGICERT INC	$412.00	$0.00	Professional Services
3112405633001	10/07/2020	10/08/2020	REI*LN RISK MNGMT	$3,708.00	$0.00	Professional Services
3113049916001	10/08/2020	10/09/2020	DTV	$2,843.88	$0.00	Utilities
3113049917001	10/07/2020	10/09/2020	LEXISNEXIS RISK SOL EP	$309.00	$0.00	Professional Services
3114903753001	10/12/2020	10/13/2020	SPROUT SOCIAL, INC	$2,960.84	$0.00	Computer, Hardware, Software and Peripherals
3126208544001	11/01/2020	11/03/2020	WIX.COM*PREMIUM-PLAN	$324.00	$0.00	Computer, Hardware, Software and Peripherals
3141458505001	12/02/2020	12/03/2020	PIPPA PODCAST SERVICES	$240.00	$0.00	Computer, Hardware, Software and Peripherals
3143910722001	12/07/2020	12/08/2020	PAYPAL	$2,535.00	$0.00	Education
3160346721001	01/13/2021	01/13/2021	ULINE	$1,548.99	$0.00	Professional Services
3162437796001	01/17/2021	01/18/2021	IN *SUPRETECH, INC.	$4,983.30	$0.00	Professional Services
3166863165001	01/25/2021	01/26/2021	VUE*COMPTIA MRKETPLCE	$740.94	$0.00	Education
3169551162001	01/30/2021	02/01/2021	ULINE	$738.50	$0.00	Professional Services
3169551163001	01/29/2021	02/01/2021	BLUEBAY OFFICE INC	$199.00	$0.00	Supplies
Elijah Crawford *5039						
3113930590001	10/10/2020	10/12/2020	D J	$20.66	$0.00	Professional Services
3117724264001	10/17/2020	10/19/2020	NYTIMES	$8.48	$0.00	Professional Services
3129850259001	11/10/2020	11/10/2020	D J	$20.66	$0.00	Professional Services
3132869616001	11/14/2020	11/16/2020	NYTIMES	$8.48	$0.00	Professional Services
3138657709001	11/25/2020	11/27/2020	IN *AWARDS AND MORE	$4,000.00	$0.00	Supplies
3145167705001	12/10/2020	12/10/2020	D J	$20.66	$0.00	Professional Services
3146708759001	12/12/2020	12/14/2020	NYTIMES	$8.48	$0.00	Professional Services
3158858758001	01/10/2021	01/11/2021	D J	$19.49	$0.00	Professional Services

3158858759001	01/09/2021	01/11/2021	NYTIMES	$8.00	$0.00	Professional Services
3166863200001	01/25/2021	01/26/2021	IN *AWARDS AND MORE	$4,250.00	$0.00	Supplies
Monica Hill *1836						
3121539449001	10/22/2020	10/26/2020	WIX.COM*NCRINTEL.ORG	$14.95	$0.00	Computer, Hardware, Software and Peripherals
3128038084001	11/05/2020	11/06/2020	BLUEBAY OFFICE INC	$423.00	$0.00	Supplies
3135066280001	11/18/2020	11/19/2020	TEEM TECHNOLOGIES	$4,000.00	$0.00	Computer, Hardware, Software and Peripherals
3143910713001	12/07/2020	12/08/2020	PAYPAL	$2,730.00	$0.00	Education
3147655407001	12/11/2020	12/15/2020	CCBC	$1,191.00	$0.00	Education
3149528810001	12/17/2020	12/18/2020	IN *SUPRETECH, INC.	$2,602.04	$0.00	Professional Services

Q12 HSEMA

PUBLIC SAFETY AND JUSTICE AGENCY							
FY 2020 REPROGRAMMING LIST							
LOCAL						Starting Budget	$5,497,378.00
FISCAL YEAR	FUND	DATE	SOAR DOC #	Program	Activity	DESCRIPTION	AMOUNT
2020	0100	9/14/2020	BJBN0917	3000	3100	FY 2020 COLA	$126,338.00
						Final Budget	$5,623,716.00

FEDERAL GRANT						Starting Budget	$131,986,292.89
FISCAL YEAR	FUND	DATE	SOAR DOC #	Program	Activity	DESCRIPTION	AMOUNT
2020	0200	10/7/2019	PABN0521	1000	1309	REPROGRAM FROM OTHER PCAS	$23,677.26
2020	0200	10/7/2019	PABN0521	1000	1309	REPROGRAM TO OTHER PCAS	($4,552.00)
2020	0200	10/7/2019	PABN0521	2000	2101	REPROGRAM FROM OTHER PCAS	$1,261,290.00
2020	0200	10/7/2019	PABN0521	2000	2113	REPROGRAM FROM OTHER PCAS	$577,497.33
2020	0200	10/7/2019	PABN0521	3000	3363	REPROGRAM FROM OTHER PCAS	$22,737.05
2020	0200	10/7/2019	PABN0521	3000	3363	REPROGRAM TO OTHER PCAS	($10,000.00)
2020	0200	10/7/2019	PABN0521	4000	4100	REPROGRAM TO OTHER PCAS	($2,071,206.91)
2020	0200	10/7/2019	PABN0521	4000	4305	REPROGRAM FROM OTHER PCAS	$958,696.36
2020	0200	10/7/2019	PABN0521	4000	4305	REPROGRAM TO OTHER PCAS	($758,139.09)
2020	0200	10/7/2019	PABN0522	1000	1338	REPROGRAM FROM 4100F	$226,606.00

2020	0200	10/7/2019	PABN0522	1000	1339	REPROGRAM FROM 4100F	$73,500.00
2020	0200	10/7/2019	PABN0522	3000	3106	REPROGRAM FROM 4100F	$292,500.00
2020	0200	10/7/2019	PABN0522	4000	4100	REPROGRAM TO OTHER PCAS	($792,606.00)
2020	0200	10/7/2019	PABN0522	5000	5101	REPROGRAM FROM 4100F	$200,000.00
2020	0200	10/10/2019	PABN0527	1000	1325	REPROGRAM FROM 4100F	$413,860.00
2020	0200	10/10/2019	PABN0527	3000	3107	REPROGRAM FROM 4100F	$71,000.00
2020	0200	10/10/2019	PABN0527	3000	3108	REPROGRAM FROM 4100F	$500,000.00
2020	0200	10/10/2019	PABN0527	3000	3109	REPROGRAM FROM 4100F	$250,000.00
2020	0200	10/10/2019	PABN0527	3000	3111	REPROGRAM FROM 4100F	$350,000.00
2020	0200	10/10/2019	PABN0527	3000	3112	REPROGRAM FROM 4100F	$500,000.00
2020	0200	10/10/2019	PABN0527	4000	4100	REPROGRAM TO OTHER PCAS	($2,084,860.00)
2020	0200	10/15/2019	PABN0528	2000	2101	REVERSE TO CORRECT PCA	($1,261,290.00)
2020	0200	10/17/2019	PABN0530	2000	2101	REPROGRAM TO CORRECT PCA	($1,078,649.99)
2020	0200	10/17/2019	PABN0530	2000	2132	REPROGRAM TO CORRECT PCA	($183,398.80)
2020	0200	10/17/2019	PABN0530	2000	2133	REPROGRAM TO CORRECT PCA	($13,000.00)
2020	0200	10/17/2019	PABN0530	4000	4100	REPROGRAM TO CORRECT PCA	$1,275,048.79

2020	0200	10/17/2019	PABN0531	2000	2132	REPROGRAM TO CORRECT PCA	($271,617.73)
2020	0200	10/17/2019	PABN0531	2000	2133	REPROGRAM TO CORRECT PCA	($175,501.20)
2020	0200	10/17/2019	PABN0531	4000	4100	REPROGRAM TO CORRECT PCA	$447,118.93
2020	0200	10/18/2019	PABN0532	2000	2182	REPROGRAM FROM OTHER OBJECTS	$1,698,393.98
2020	0200	10/18/2019	PABN0532	2000	2182	REPROGRAM TO OTHER PCAS	($377,296.00)
2020	0200	10/18/2019	PABN0532	2000	2183	REPROGRAM FROM OTHER OBJECTS	$326,866.00
2020	0200	10/18/2019	PABN0532	3000	3105	REPROGRAM FROM OTHER PCAS	$76,104.50
2020	0200	10/18/2019	PABN0532	4000	4100	REPROGRAM TO OTHER PCAS	($1,724,068.48)
2020	0200	10/22/2019	PABN0534	2000	2101	REPROGRAM FROM 4100F FIX	$1,078,649.99
2020	0200	10/22/2019	PABN0534	2000	2132	REPROGRAM FROM 4100F FIX	$183,398.80
2020	0200	10/22/2019	PABN0534	2000	2133	REPROGRAM FROM 4100F FIX	$13,000.00
2020	0200	10/22/2019	PABN0534	4000	4100	REPROGRAM TO 2101F 2132F 2133F	($1,275,048.79)
2020	0200	10/22/2019	PABN0535	2000	2132	REPROGRAM FROM 4100F FIX	$271,617.73
2020	0200	10/22/2019	PABN0535	2000	2133	REPROGRAM FROM 4100F FIX	$175,501.20
2020	0200	10/22/2019	PABN0535	4000	4100	REPROGRAM TO 2132F & 2133F	($447,118.93)
2020	0200	10/24/2019	PABN0536	4000	4100	TO CORRECT BATCH #528 PCA 2101	$1,261,290.00

2020	0200	10/30/2019	PABN0537	1000	1306	REPROGRAM FROM 4100F AND 2183F	$80,000.00
2020	0200	10/30/2019	PABN0537	2000	2183	REPROGRAM FROM 4100F AND 2183F	$80,331.08
2020	0200	10/30/2019	PABN0537	2000	2183	REPROGRAM TO OTHER PCAS	($38,789.81)
2020	0200	10/30/2019	PABN0537	4000	4100	REPROGRAM TO OTHER PCAS	($163,169.27)
2020	0200	10/30/2019	PABN0537	5000	5101	REPROGRAM FROM 4100F AND 2183F	$41,628.00
2020	0200	10/30/2019	PABN0539	2000	2182	REPROGRAM TO 4100F & 3115F	($1,516,992.53)
2020	0200	10/30/2019	PABN0539	3000	3115	REPROGRAM FROM 2182F	$36,072.58
2020	0200	10/30/2019	PABN0539	4000	4100	REPROGRAM FROM 2182F	$1,480,919.95
2020	0200	11/7/2019	PABN0541	2000	2101	REPROGRAM FROM OTHER PCAS	$304,963.37
2020	0200	11/7/2019	PABN0541	2000	2101	REPROGRAM TO OTHER PCAS	($122,323.36)
2020	0200	11/7/2019	PABN0541	2000	2308	REPROGRAM FROM OTHER PCAS	$128,919.04
2020	0200	11/7/2019	PABN0541	2000	2308	REPROGRAM TO OTHER PCAS	($13,446.16)
2020	0200	11/7/2019	PABN0541	4000	4100	REPROGRAM TO OTHER PCAS	($302,789.24)
2020	0200	11/7/2019	PABN0541	4000	4402	REPROGRAM FROM OTHER PCAS	$34,676.35
2020	0200	11/7/2019	PABN0541	4000	4402	REPROGRAM TO OTHER PCAS	($30,000.00)
2020	0200	11/7/2019	PABN0542	5000	5101	REPROGRAM FROM 0409	$41,628.00

2020	0200	11/7/2019	PABN0542	5000	5101	REPROGRAM TO 0702 AND 0711	($41,628.00)
2020	0200	11/8/2019	PABN0543	4000	4100	REPROGRAM FROM 0506	$2,500,000.00
2020	0200	11/8/2019	PABN0543	4000	4100	REPROGRAM TO 0702	($2,500,000.00)
2020	0200	11/7/2019	PABN0544	1000	1306	REPROGRAM FROM OTHER COBJ	$52,828.67
2020	0200	11/7/2019	PABN0544	1000	1306	REPROGRAM TO OTHER COBJ	($56,702.30)
2020	0200	11/7/2019	PABN0544	4000	4100	REPROGRAM FROM OTHER COBJ	$3,873.63
2020	0200	11/22/2019	PABN0546	2000	2183	REPROGRAM FROM 4100F & 2183F	$14,934.10
2020	0200	11/22/2019	PABN0546	2000	2183	REPROGRAM TO 2183 OTHER COBJ	($6,474.57)
2020	0200	11/22/2019	PABN0546	4000	4100	REPROGRAM TO 2183	($8,459.53)
2020	0200	11/22/2019	PABN0547	2000	2182	REPROGRAM TO 3105F & 4100F	($5,097.75)
2020	0200	11/22/2019	PABN0547	3000	3105	REPROGRAM FROM OTHER COBJ	$53,124.00
2020	0200	11/22/2019	PABN0547	3000	3105	REPROGRAM TO OTHER COBJ & 4100	($53,124.00)
2020	0200	11/22/2019	PABN0547	4000	4100	REPROGRAM FROM OTHER COBJ	$5,097.75
2020	0200	11/27/2019	PABN0570	2000	2133	REPROGRAM FROM 4100F	$175,644.00
2020	0200	11/27/2019	PABN0570	2000	2133	REPROGRAM TO OTHER PCAS	($13,000.00)
2020	0200	11/27/2019	PABN0570	2000	2183	REPROGRAM FROM 4100F	$306,040.00
2020	0200	11/27/2019	PABN0570	4000	4100	REPROGRAM TO OTHER PCAS	($468,684.00)

2020	0200	12/4/2019	BHBN0571	2000	2100	BUDGET ESTABLISHMENT	$803,443.95
2020	0200	12/23/2019	BHBN0572	4000	4100	BUDGET INCREASE	$559,694.49
2020	0200	12/23/2019	PABN0573	2000	2132	REPROGRAM FROM 4100F & 2308F	$114,649.20
2020	0200	12/23/2019	PABN0573	2000	2308	REPROGRAM FROM 4100F & 2308F	$9,000.00
2020	0200	12/23/2019	PABN0573	2000	2308	REPROGRAM TO 2132F & 2308F	($9,000.00)
2020	0200	12/23/2019	PABN0573	4000	4100	REPROGRAM TO 2132F & 2308F	($112,649.20)
2020	0200	12/23/2019	PABN0573	4000	4402	REPROGRAM TO 2132F & 2308F	($2,000.00)
2020	0200	12/31/2019	PABN0574	4000	4100	REPROGRAM TO 4306F	($715,830.00)
2020	0200	12/31/2019	PABN0574	4000	4306	REPROGRAM FROM 4100F	$715,830.00
2020	0200	12/31/2019	PABN0575	3000	3116	REPROGRAM FROM 4100F	$550,000.00
2020	0200	12/31/2019	PABN0575	4000	4100	REPROGRAM TO 3116F	($550,000.00)
2020	0200	1/6/2020	BHBN0576	2000	2100	BUDGET ESTABLISHMENT	$818,078.94
2020	0200	1/14/2020	PABN0577	2000	2182	REPROGRAM TO 4100F, 0506	($360.00)
2020	0200	1/14/2020	PABN0577	4000	4100	REPROGRAM FROM 2182F, 0147	$360.00
2020	0200	1/14/2020	PABN0578	3000	3109	REPROGRAM FROM 0702	$200,000.00
2020	0200	1/14/2020	PABN0578	3000	3109	REPROGRAM TO 0402 & 0409	($200,000.00)
2020	0200	1/16/2020	PABN0579	1000	1312	REPROGRAM TO 3113F	($180,720.69)
2020	0200	1/16/2020	PABN0579	3000	3113	REPROGRAM FROM 1312F	$186,359.00
2020	0200	1/16/2020	PABN0579	4000	4100	REPROGRAM TO 3113F	($5,638.31)

2020	0200	1/21/2020	BHBN0580	4000	4100	BUDGET REDUCTION TO AWARD	($26,630,789.62)
2020	0200	1/21/2020	PABN0581	4000	4306	REPROGRAM FROM 0409	$209,680.70
2020	0200	1/21/2020	PABN0581	4000	4306	REPROGRAM TO 0702	($209,680.70)
2020	0200	1/27/2020	PABN0582	2000	2113	REPROGRAM TO 2182F	($127,800.00)
2020	0200	1/27/2020	PABN0582	2000	2182	REPROGRAM FROM 4100F & 2113F	$1,765,796.00
2020	0200	1/27/2020	PABN0582	2000	2182	REPROGRAM TO OTHER COBJ	($405,796.00)
2020	0200	1/27/2020	PABN0582	4000	4100	REPROGRAM TO 2182F	($1,232,200.00)
2020	0200	2/11/2020	BHBN0583	4000	4100	BUDGET ESTABLISHMENT	$1,138,790.00
2020	0200	2/18/2020	PABN0584	2000	2113	REPROGRAM FROM OTHER PCAS	$152,201.66
2020	0200	2/18/2020	PABN0584	2000	2113	REPROGRAM TO OTHER PCAS	($152,201.66)
2020	0200	2/18/2020	PABN0584	2000	2182	REPROGRAM FROM OTHER PCAS	$366,155.06
2020	0200	2/18/2020	PABN0584	2000	2182	REPROGRAM TO OTHER PCAS	($366,155.06)
2020	0200	2/18/2020	PABN0584	3000	3109	REPROGRAM FROM OTHER PCAS	$26,500.00
2020	0200	2/18/2020	PABN0584	3000	3109	REPROGRAM TO OTHER PCAS	($26,500.00)
2020	0200	2/18/2020	PABN0584	3000	3116	REPROGRAM TO OTHER PCAS	($40,585.00)
2020	0200	2/18/2020	PABN0584	4000	4100	REPROGRAM FROM OTHER PCAS	$40,585.00
2020	0200	2/24/2020	BHBN0585	4000	4100	BUDGET REDUCTION	($10,000,000.00)
2020	0200	2/24/2020	BHBN0586	4000	4100	BUDGET REDUCTION	($50,000.00)
2020	0200	2/26/2020	BHBN0588	2000	2100	BUDGET ESTABLISHMENT	$24,433.55

2020	0200	2/26/2020	BHBN0589	2000	2100	BUDGET ESTABLISHMENT	$1,164,475.75
2020	0200	2/26/2020	BHBN0590	2000	2100	BUDGET ESTABLISHMENT	$43,490.91
2020	0200	2/26/2020	BHBN0591	2000	2100	BUDGET ESTABLISHMENT	$1,032,949.04
2020	0200	2/26/2020	PABN0587	2000	2132	REPROGRAM FROM OTHER PCAS	$145,040.00
2020	0200	2/26/2020	PABN0587	4000	4100	REPROGRAM TO OTHER PCAS	($145,040.00)
2020	0200	2/26/2020	PABN0587	4000	4305	REPROGRAM FROM OTHER PCAS	$5,000.00
2020	0200	2/26/2020	PABN0587	4000	4305	REPROGRAM TO OTHER PCAS	($5,000.00)
2020	0200	2/26/2020	PABN0587	4000	4402	REPROGRAM FROM OTHER PCAS	$10,000.00
2020	0200	2/26/2020	PABN0587	4000	4402	REPROGRAM TO OTHER PCAS	($10,000.00)
2020	0200	3/2/2020	PABN0590	3000	3105	REPROGRAM FROM 4100F	$40,757.43
2020	0200	3/2/2020	PABN0590	4000	4100	REPROGRAM TO 3105F	($40,757.43)
2020	0200	3/4/2020	PABN0591	4000	4305	REPROGRAM FROM 0409	$10,000.00
2020	0200	3/4/2020	PABN0591	4000	4305	REPROGRAM TO 0308	($10,000.00)
2020	0200	3/9/2020	PABN0594	1000	1309	REPROGRAM TO OTHER PCAS	($5,000.00)
2020	0200	3/9/2020	PABN0594	2000	2103	REPROGRAM FROM OTHER PCAS	$6,000.00
2020	0200	3/9/2020	PABN0594	2000	2103	REPROGRAM TO OTHER PCAS	($388,346.52)
2020	0200	3/9/2020	PABN0594	2000	2104	REPROGRAM FROM OTHER PCAS	$20,049.67

2020	0200	3/9/2020	PABN0594	2000	2104	REPROGRAM TO OTHER PCAS	($1,420.73)
2020	0200	3/9/2020	PABN0594	2000	2313	REPROGRAM FROM OTHER PCAS	$430,820.74
2020	0200	3/9/2020	PABN0594	2000	2313	REPROGRAM TO OTHER PCAS	($185,465.00)
2020	0200	3/9/2020	PABN0594	4000	4100	REPROGRAM FROM OTHER PCAS	$123,361.84
2020	0200	4/10/2020	PABN0600	2000	2182	REPROGRAM TO 4100F	($58,788.00)
2020	0200	4/10/2020	PABN0600	4000	4100	REPROGRAM FROM 2182F	$58,788.00
2020	0200	4/15/2020	PABN0601	2000	2182	REPROGRAM FROM 0409	$285,000.00
2020	0200	4/20/2020	PABN0602	4000	4FA0	REPROGRAM FROM 0408	$10,000.00
2020	0200	5/4/2020	BHBN0603	1000	1320	GRANT BUDGET REDUCTION	($33,000.00)
2020	0200	5/4/2020	PABN0604	4000	4FA0	REPROGRAM FROM 1320F	$30,000.00
2020	0200	5/26/2020	BHBN0605	4000	4100	BUDGET MODIFICATION-INCREASE	$1,500,000.00
2020	0200	5/26/2020	PABN0606	2000	2101	REPROGRAM FROM 2101	$480.00
2020	0200	5/26/2020	PABN0606	2000	2101	REPROGRAM TO 2101 AND 4100	($155,844.00)
2020	0200	5/26/2020	PABN0606	4000	4100	REPROGRAM FROM 4305 AND 2101	$224,682.00
2020	0200	5/26/2020	PABN0606	4000	4305	REPROGRAM TO 2101 AND 4100	($69,318.00)
2020	0200	6/1/2020	BHBN0603	3000	3100	GRANT BUDGET REDUCTION	($442,000.00)
2020	0200	6/1/2020	PABN0601	2000	2182	REPROGRAM TO 0702	($285,000.00)
2020	0200	6/1/2020	PABN0602	4000	4FA0	REPROGRAM TO 0209	($10,000.00)

2020	0200	6/1/2020	PABN0604	1000	1320	REPROGRAM TO 4FA0F	($30,000.00)
2020	0200	6/15/2020	PABN0608	1000	1306	REPROGRAM FROM OTHER COBJ	$19,925.00
2020	0200	6/15/2020	PABN0608	1000	1306	REPROGRAM TO 0409	($19,925.00)
2020	0200	6/15/2020	PABN0609	2000	2182	REPROGRAM TO 4100F	($233,046.00)
2020	0200	6/15/2020	PABN0609	4000	4100	REPROGRAM FROM 2182F	$233,046.00
2020	0200	6/17/2020	PABN0610	3000	3109	REPROGRAM FROM 0506	$665,000.00
2020	0200	6/17/2020	PABN0610	4000	4100	REPROGRAM TO 0409	($665,000.00)
2020	0200	6/19/2020	PABN0611	4000	4306	REPROGRAM FROM 0409	$200,000.00
2020	0200	6/19/2020	PABN0611	4000	4306	REPROGRAM TO 0702	($200,000.00)
2020	0200	6/22/2020	PABN0622	2000	2113	REPROGRAM TO 4100F	($38,340.00)
2020	0200	6/22/2020	PABN0622	4000	4100	REPROGRAM FROM 2113F	$38,340.00
2020	0200	6/29/2020	BHBN0613	1000	1306	BUDGET ESTABLISHMENT	$51,465.68
2020	0200	6/29/2020	BHBN0613	1000	1309	BUDGET ESTABLISHMENT	$31,740.45
2020	0200	6/29/2020	BHBN0613	1000	1310	BUDGET ESTABLISHMENT	$53,370.24
2020	0200	6/29/2020	BHBN0613	1000	1320	BUDGET ESTABLISHMENT	$125,952.57
2020	0200	6/29/2020	BHBN0613	2000	2100	BUDGET ESTABLISHMENT	$27,188.38
2020	0200	6/29/2020	BHBN0613	2000	2113	BUDGET ESTABLISHMENT	$25,341.82
2020	0200	6/29/2020	BHBN0613	2000	2134	BUDGET ESTABLISHMENT	$30,222.92
2020	0200	6/29/2020	BHBN0613	3000	3100	BUDGET ESTABLISHMENT	$294,951.44

2020	0200	6/29/2020	BHBN0613	4000	4101	BUDGET ESTABLISHMENT	$27,514.53
2020	0200	6/29/2020	BHBN0613	4000	4305	BUDGET ESTABLISHMENT	$15,406.72
2020	0200	6/29/2020	BHBN0613	4000	4402	BUDGET ESTABLISHMENT	$58,017.26
2020	0200	6/29/2020	BHBN0613	4000	4FA0	BUDGET ESTABLISHMENT	$44,083.20
2020	0200	6/29/2020	BHBN0613	4000	4FA1	BUDGET ESTABLISHMENT	$69,999.74
2020	0200	6/29/2020	BHBN0613	4000	4FA2	BUDGET ESTABLISHMENT	$22,363.05
2020	0200	7/8/2020	BHBN0708	4000	4100	FY20 BN0 BUDGET INCREASE REQ	$350,507.00
2020	0200	7/21/2020	BHBN0614	4000	4100	BUDGET ESTABLISHMENT	$64,444.54
2020	0200	7/21/2020	PABN0615	2000	2132	REPROGRAM FROM 0402 &0409	$16,991.76
2020	0200	7/21/2020	PABN0615	2000	2132	REPROGRAM TO 0111	($16,991.76)
2020	0200	7/21/2020	PABN0615	4000	4305	REPROGRAM FROM 0409	$180,000.00
2020	0200	7/21/2020	PABN0615	4000	4305	REPROGRAM TO 0702	($180,000.00)
2020	0200	7/21/2020	PABN0616	2000	2182	REPROGRAM FROM 0408 & 0702	$59,551.22
2020	0200	7/21/2020	PABN0616	2000	2182	REPROGRAM TO 0111	($59,551.22)
2020	0200	7/27/2020	BHBN0625	4000	4100	BUDGET INCREASE	$10,000,000.00
2020	0200	7/29/2020	PABN0626	3000	3109	REPROGRAM FROM 4100F & 3109	$264,167.20
2020	0200	7/29/2020	PABN0626	3000	3109	REPROGRAM TO 0041 & 702	($4,967.20)
2020	0200	7/29/2020	PABN0626	4000	4100	REPROGRAM TO 3109F 0041 & 702	($259,200.00)
2020	0200	8/12/2020	BHBN0627	4000	4100	BUDGET INCREASE	$164,748.63

2020	0200	8/24/2020	BHBN0628	4000	4100	GRANT BUDGET INCREASE	$38,559,311.26
2020	0200	9/8/2020	PABN0630	4000	4100	REPROGRAM FROM 0506	$1,000,000.00
2020	0200	9/8/2020	PABN0630	4000	4100	REPROGRAM TO 0702	($1,000,000.00)
2020	0200	9/8/2020	PABN0631	3000	3106	REPROGRAM FROM 4100F, 0506	$378,125.00
2020	0200	9/8/2020	PABN0631		4100	REPROGRAM TO 3106F, 0409	($378,125.00)
2020	0200	9/8/2020	PABN0632	2000	2101	REPROGRAM TO 4100F	($20,000.00)
2020	0200	9/8/2020	PABN0632	2000	2104	REPROGRAM TO 4100F	($51,837.00)
2020	0200	9/8/2020	PABN0632	2000	2313	REPROGRAM TO 4100F	($75,253.00)
2020	0200	9/8/2020	PABN0632	4000	4100	REPROGRAM FROM 2101,2104,2313	$147,090.00
2020	0200	9/9/2020	BHBN0634	4000	4100	BUDGET INCREASE	$6,116,981.52
2020	0200	9/16/2020	BHBN0635	4000	4100	GRANT BUDGET INCREASE	$2,986,233.32
2020	0200	9/23/2020	BHBN0636	4000	4100	BUDGET MODIFICATION-INCREASE	$920,636.24
2020	0200	9/30/2020	BHBN0638	4000	4100	FY 2020 BUDGET INCREASE	$16,248,100.89
2020	0200	9/30/2020	BHBN0648	4000	4100	BUDGET INCREASE	$74,939,543.60
2020	0200	9/30/2020	BHBN0649	4000	4100	BUDGET INCREASE	$160,000,000.00
2020	0200	9/30/2020	BHBN0659	4000	4100	BUDGET REDUCTION	($1,138,790.00)
2020	0200	9/30/2020	BHBN0661	2000	2100	BUDGET DECREASE	($24,433.55)
2020	0200	9/30/2020	BHBN0662	2000	2100	BUDGET DECREASE	($35,909.91)
2020	0200	9/30/2020	BHBN0663	2000	2100	GRANT BUDGET DECREASE	($1,826,681.22)
2020	0200	9/30/2020	BHBN0664	4000	4100	BUDGET DECREASE	($2,000,000.00)
2020	0200	9/30/2020	BHBN0665	2000	2100	BUDGET DECREASE	($67,414.47)
2020	0200	9/30/2020	BHBN0666	4000	4100	BUDGET DECREASE	($3,286,413.02)
2020	0200	9/30/2020	BHBN0667	2000	2100	BUDGET DECREASE	($48,424.91)
2020	0200	9/30/2020	BHBN0668	2000	2100	BUDGET DECREASE	($107,172.97)

2020	0200	9/30/2020	BHBN0669	4000	4100	BUDGET DECREASE	($10,000,000.00)
2020	0200	9/30/2020	BHBN0670	2000	2100	BUDGET DECREASE	($649,329.54)
2020	0200	9/30/2020	BHBN0671	4000	4100	BUDGET DECREASE	($1,000,000.00)
2020	0200	9/30/2020	BHBN0672	4000	4100	BUDGET DECREASE	($685,301.16)
2020	0200	9/30/2020	BHBN0673	4000	4100	BUDGET DECREASE	($1,000,998.36)
2020	0200	9/30/2020	BHBN0674	2000	2100	BUDGET DECREASE	($789,442.71)
2020	0200	9/30/2020	BHBN0675	2000	2100	BUDGET DECREASE	($59,009.31)
2020	0200	9/30/2020	BHBN0676	2000	2100	BUDGET DECREASE	($150,000.00)
2020	0200	9/30/2020	BHBN0677	2000	2100	BUDGET DECREASE	($22,622.06)
2020	0200	9/30/2020	BJBN0678	4000	4100	FY2020 GRANT CLOSEOUT	($894,723.67)
2020	0200	9/30/2020	BJBN0679	4000	4100	FY20 GRANT CLOSEOUT	($141,979.69)
2020	0200	9/30/2020	BJBN0680	2000	2100	FY 2020 GRANT CLOSEOUT	($101,736.23)
2020	0200	9/30/2020	BJBN0681	1000	1306	FY 2020 GRANT CLOSEOUT	($50,763.22)
2020	0200	9/30/2020	BJBN0681	1000	1309	FY 2020 GRANT CLOSEOUT	($8,472.51)
2020	0200	9/30/2020	BJBN0681	1000	1310	FY 2020 GRANT CLOSEOUT	($28,915.67)
2020	0200	9/30/2020	BJBN0681	1000	1320	FY 2020 GRANT CLOSEOUT	($253,639.10)
2020	0200	9/30/2020	BJBN0681	2000	2100	FY 2020 GRANT CLOSEOUT	($21,759.68)
2020	0200	9/30/2020	BJBN0681	2000	2101	FY 2020 GRANT CLOSEOUT	($34,746.00)
2020	0200	9/30/2020	BJBN0681	2000	2102	FY 2020 GRANT CLOSEOUT	($26,806.61)
2020	0200	9/30/2020	BJBN0681	2000	2113	FY 2020 GRANT CLOSEOUT	($18,734.97)
2020	0200	9/30/2020	BJBN0681	2000	2134	FY 2020 GRANT CLOSEOUT	($10,254.08)

2020	0200	9/30/2020	BJBN0681	3000	3100	FY 2020 GRANT CLOSEOUT	($219,994.49)
2020	0200	9/30/2020	BJBN0681	4000	4305	FY 2020 GRANT CLOSEOUT	($80,100.90)
2020	0200	9/30/2020	BJBN0681	4000	4402	FY 2020 GRANT CLOSEOUT	($271,219.10)
2020	0200	9/30/2020	BJBN0681	4000	4FA0	FY 2020 GRANT CLOSEOUT	($334,882.94)
2020	0200	9/30/2020	BJBN0681	4000	4FA1	FY 2020 GRANT CLOSEOUT	($22,057.54)
2020	0200	9/30/2020	BJBN0681	4000	4FA2	FY 2020 GRANT CLOSEOUT	($451.89)
2020	0200	9/30/2020	BJBN0682	1000	1306	FY 2020 GRANT CLOSEOUT	($312,976.46)
2020	0200	9/30/2020	BJBN0682	1000	1309	FY 2020 GRANT CLOSEOUT	($141,697.61)
2020	0200	9/30/2020	BJBN0682	1000	1325	BN0 FY 2020 GRANTS	($245,600.92)
2020	0200	9/30/2020	BJBN0682	2000	2101	BN0 FY 2020 GRANTS	($733,356.81)
2020	0200	9/30/2020	BJBN0682	2000	2103	BN0 FY 2020 GRANTS	($163,158.85)
2020	0200	9/30/2020	BJBN0682	2000	2104	BN0 FY 2020 GRANTS	($19,272.63)
2020	0200	9/30/2020	BJBN0682	2000	2105	BN0 FY 2020 GRANTS	($258,481.40)
2020	0200	9/30/2020	BJBN0682	2000	2106	BN0 FY 2020 GRANTS	($210,097.70)
2020	0200	9/30/2020	BJBN0682	2000	2113	BN0 FY 2020 GRANTS	($362,667.34)
2020	0200	9/30/2020	BJBN0682	2000	2132	BN0 FY 2020 GRANTS	($215,468.77)
2020	0200	9/30/2020	BJBN0682	2000	2133	FY 2020 GRANT CLOSEOUT	($17,514.06)
2020	0200	9/30/2020	BJBN0682	2000	2182	FY 2020 GRANT CLOSEOUT	($1,872,253.67)
2020	0200	9/30/2020	BJBN0682	2000	2183	FY 2020 GRANT CLOSEOUT	($305,373.78)
2020	0200	9/30/2020	BJBN0682	2000	2308	FY 2020 GRANT CLOSEOUT	($203,866.77)

2020	0200	9/30/2020	BJBN0682	2000	2313	FY 2020 GRANT CLOSEOUT	($241,667.97)
2020	0200	9/30/2020	BJBN0682	3000	3105	FY 2020 GRANT CLOSEOUT	($71,000.00)
2020	0200	9/30/2020	BJBN0682	3000	3107	FY 2020 GRANT CLOSEOUT	($63,171.50)
2020	0200	9/30/2020	BJBN0682	3000	3108	FY 2020 GRANT CLOSEOUT	($500,000.00)
2020	0200	9/30/2020	BJBN0682	3000	3109	FY 2020 GRANT CLOSEOUT	($404,606.24)
2020	0200	9/30/2020	BJBN0682	3000	3111	FY 2020 GRANT CLOSEOUT	($291,283.13)
2020	0200	9/30/2020	BJBN0682	3000	3112	FY 2020 GRANT CLOSEOUT	($500,000.00)
2020	0200	9/30/2020	BJBN0682	3000	3113	FY 2020 GRANT CLOSEOUT	($119,886.31)
2020	0200	9/30/2020	BJBN0682	3000	3116	FY 2020 GRANT CLOSEOUT	($450,328.00)
2020	0200	9/30/2020	BJBN0682	3000	3363	FY 2020 GRANT CLOSEOUT	($37,547.07)
2020	0200	9/30/2020	BJBN0682	4000	4100	FY 2020 GRANT CLOSEOUT	($3,815,061.99)
2020	0200	9/30/2020	BJBN0682	4000	4124	FY 2020 GRANT CLOSEOUT	($5,000.00)
2020	0200	9/30/2020	BJBN0682	4000	4305	FY 2020 GRANT CLOSEOUT	($517,640.82)
2020	0200	9/30/2020	BJBN0682	4000	4402	FY 2020 GRANT CLOSEOUT	($243,194.27)
2020	0200	9/30/2020	BJBN0682	4000	4403	FY 2020 GRANT CLOSEOUT	($116,062.55)
2020	0200	9/30/2020	BJBN0683	1000	1338	FY 2020 GRANT CLOSEOUT	($5,841.82)

2020	0200	9/30/2020	BJBN0683	1000	1339	FY 2020 GRANT CLOSEOUT	($55,164.75)
2020	0200	9/30/2020	BJBN0683	2000	2132	FY 2020 GRANT CLOSEOUT	($50,743.38)
2020	0200	9/30/2020	BJBN0683	1000	3106	FY 2020 GRANT CLOSEOUT	($61,073.47)
2020	0200	9/30/2020	BJBN0684	1000	1306	FY 2020 GRANT CLOSEOUT	($44,808.70)
2020	0200	9/30/2020	BJBN0684	1000	1309	FY 2020 GRANT CLOSEOUT	($31,604.98)
2020	0200	9/30/2020	BJBN0684	1000	1310	FY 2020 GRANT CLOSEOUT	($17,561.89)
2020	0200	9/30/2020	BJBN0684	1000	1320	FY 2020 GRANT CLOSEOUT	($50,770.11)
2020	0200	9/30/2020	BJBN0684	2000	2100	FY 2020 GRANT CLOSEOUT	($5,850.39)
2020	0200	9/30/2020	BJBN0684	2000	2102	FY 2020 GRANT CLOSEOUT	($27,100.12)
2020	0200	9/30/2020	BJBN0684	2000	2113	FY 2020 GRANT CLOSEOUT	($10,256.27)
2020	0200	9/30/2020	BJBN0684	2000	2134	FY 2020 GRANT CLOSEOUT	($10,015.16)
2020	0200	9/30/2020	BJBN0684	3000	3100	FY 2020 GRANT CLOSEOUT	($77,030.42)
2020	0200	9/30/2020	BJBN0684		4101	FY 2020 GRANT CLOSEOUT	($13,684.75)
2020	0200	9/30/2020	BJBN0684	4000	4305	FY 2020 GRANT CLOSEOUT	($41,484.16)
2020	0200	9/30/2020	BJBN0684	4000	4402	FY 2020 GRANT CLOSEOUT	($24,669.66)
2020	0200	9/30/2020	BJBN0684	4000	4FA0	FY 2020 GRANT CLOSEOUT	($78,272.22)

2020	0200	9/30/2020	BJBN0684	4000	4FA1	FY 2020 GRANT CLOSEOUT	($59,713.64)
2020	0200	9/30/2020	BJBN0684	4000	4FA2	FY 2020 GRANT CLOSEOUT	($18,124.13)
2020	0200	9/30/2020	BJBN0685	1000	1306	FY 2020 GRANT CLOSEOUT	($24,293.77)
2020	0200	9/30/2020	BJBN0685	2000	2182	FY 2020 GRANT CLOSEOUT	($593,410.48)
2020	0200	9/30/2020	BJBN0685	2000	2183	FY 2020 GRANT CLOSEOUT	($104,315.25)
2020	0200	9/30/2020	BJBN0685	3000	3105	FY 2020 GRANT CLOSEOUT	($63,039.59)
2020	0200	9/30/2020	BJBN0685	3000	3106	FY 2020 GRANT CLOSEOUT	($378,125.00)
2020	0200	9/30/2020	BJBN0685	3000	3109	FY 2020 GRANT CLOSEOUT	($665,000.00)
2020	0200	9/30/2020	BJBN0685	4000	4100	FY 2020 GRANT CLOSEOUT	($10,357,019.82)
2020	0200	9/30/2020	BJBN0685	4000	4124	FY 2020 GRANT CLOSEOUT	($204,265.06)
2020	0200	9/30/2020	BJBN0685	5000	5101	FY 2020 GRANT CLOSEOUT	($36,321.69)
2020	0200	9/30/2020	BJBN0727	4000	4100	FY 2020 GRANT CLOSEOUT	##############
2020	0200	9/30/2020	BJBN076M	4000	4100	COVID19 PUBLIC ASSISTANCE	$76,806,930.95
2020	0200	9/30/2020	PABN0646	2000	2100	REPROGRAM FROM 0111	$5,247.65
2020	0200	9/30/2020	PABN0646	2000	2100	REPROGRAM TO 012 & 015	($5,247.65)
2020	0200	9/30/2020	PABN0678	1000	1338	REPROGRAM TO 4100F	($160,000.00)
2020	0200	9/30/2020	PABN0678	2000	2132	REPROGRAM TO 4100F	($200,000.00)

2020	0200	9/30/2020	PABN0678	4000	4100	REPROGRAM FROM OTHER PCAS	$700,000.00
2020	0200	9/30/2020	PABN0678	4000	4306	REPROGRAM TO 4100F	($340,000.00)
						Final Budget	**$257,857,379.88**

INTRA DISTRICT						**Starting Budget**	**$0.00**
FISCAL YEAR	**FUND**	**DATE**	**SOAR DOC #**	**Program**	**Activity**	**DESCRIPTION**	**AMOUNT**
2020	0700	8/11/2020	BJBNSEP1	1000	1306	BN0 2ND QTR EP0 REIMBURSEMENT	1,517.70
2020	0700	8/11/2020	BJBNSEP1	1000	1309	BN0 2ND QTR EP0 REIMBURSEMENT	683.42
2020	0700	8/11/2020	BJBNSEP1	1000	1310	BN0 2ND QTR EP0 REIMBURSEMENT	2,253.10
2020	0700	8/11/2020	BJBNSEP1	1000	1320	BN0 2ND QTR EP0 REIMBURSEMENT	3,845.82
2020	0700	8/11/2020	BJBNSEP1	1000	1325	BN0 2ND QTR EP0 REIMBURSEMENT	1,067.48
2020	0700	8/11/2020	BJBNSEP1	2000	2100	BN0 2ND QTR EP0 REIMBURSEMENT	642.80
2020	0700	8/11/2020	BJBNSEP1	2000	2103	BN0 2ND QTR EP0 REIMBURSEMENT	137.18
2020	0700	8/11/2020	BJBNSEP1	2000	2113	BN0 2ND QTR EP0 REIMBURSEMENT	1,287.35
2020	0700	8/11/2020	BJBNSEP1	2000	2133	BNO 2ND QTR EP0 REIMBURSEMENT	141.43
2020	0700	8/11/2020	BJBNSEP1	2000	2134	BN0 2ND QTR EP0 REIMBURSEMENT	1,265.96
2020	0700	8/11/2020	BJBNSEP1	2000	2182	BN0 2ND QTR EP0 REIMBURSEMENT	686.47
2020	0700	8/11/2020	BJBNSEP1	3000	3100	BN0 2ND QTR EP0 REIMBURSEMENT	8,722.32

2020	0700	8/11/2020	BJBNSEP1	3000	3111	BN0 2ND QTR EP0 REIMBURSEMENT	831.13
2020	0700	8/11/2020	BJBNSEP1	3000	3363	BN0 2ND QTR EP0 REIMBURSEMENT	208.33
2020	0700	8/11/2020	BJBNSEP1	4000	4100	BN0 2ND QTR EP0 REIMBURSEMENT	568.28
2020	0700	8/11/2020	BJBNSEP1	4000	4101	BN0 2ND QTR EP0 REIMBURSEMENT	593.48
2020	0700	8/11/2020	BJBNSEP1	4000	4305	BN0 2ND QTR EP0 REIMBURSEMENT	2,444.26
2020	0700	8/11/2020	BJBNSEP1	4000	4402	BN0 2ND QTR EP0 REIMBURSEMENT	1,534.58
2020	0700	8/11/2020	BJBNSEP1	4000	4FA0	BN0 2ND QTR EP0 REIMBURSEMENT	3,863.97
2020	0700	8/11/2020	BJBNSEP1	4000	4FA1	BN0 2ND QTR EP0 REIMBURSEMENT	2,186.00
2020	0700	8/11/2020	BJBNSEP1	4000	4FA2	BN0 2ND QTR EP0 REIMBURSEMENT	1,613.42
2020	0700	8/31/2020	BJBNEP15	3000	3100	COVID REIMBURSEMENT	1,941,174.36
2020	0700	9/30/2020	BJBN0020	1000	1040	3RD QTR EP0 REIMBURSEMENT	1,881.00
2020	0700	9/30/2020	BJBN0020	1000	1306	3RD QTR EP0 REIMBURSEMENT	1,970.60
2020	0700	9/30/2020	BJBN0020	1000	1310	3RD QTR EP0 REIMBURSEMENT	1,895.12
2020	0700	9/30/2020	BJBN0020	1000	1320	3RD QTR EP0 REIMBURSEMENT	5,368.00
2020	0700	9/30/2020	BJBN0020	1000	1325	3RD QTR EP0 REIMBURSEMENT	1,670.09
2020	0700	9/30/2020	BJBN0020	2000	2101	3RD QTR EP0 REIMBURSEMENT	1,419.40
2020	0700	9/30/2020	BJBN0020	2000	2103	3RD QTR EP0 REIMBURSEMENT	1,785.60

2020	0700	9/30/2020	BJBN0020	2000	2113	3RD QTR EP0 REIMBURSEMENT	3,941.18
2020	0700	9/30/2020	BJBN0020	2000	2132	3RD QTR EP0 REIMBURSEMENT	3,130.22
2020	0700	9/30/2020	BJBN0020	2000	2182	3RD QTR EP0 REIMBURSEMENT	3,264.02
2020	0700	9/30/2020	BJBN0020	2000	2308	3RD QTR EP0 REIMBURSEMENT	714.99
2020	0700	9/30/2020	BJBN0020	2000	2313	3RD QTR EP0 REIMBURSEMENT	1,960.76
2020	0700	9/30/2020	BJBN0020	3000	3100	3RD QTR EP0 REIMBURSEMENT	13,003.36
2020	0700	9/30/2020	BJBN0020	3000	3111	3RD QTR EP0 REIMBURSEMENT	574.74
2020	0700	9/30/2020	BJBN0020	3000	3363	3RD QTR EP0 REIMBURSEMENT	416.65
2020	0700	9/30/2020	BJBN0020	4000	4100	3RD QTR EP0 REIMBURSEMENT	1,132.71
2020	0700	9/30/2020	BJBN0020	4000	4305	3RD QTR EP0 REIMBURSEMENT	4,940.87
2020	0700	9/30/2020	BJBN0020	4000	4402	3RD QTR EP0 REIMBURSEMENT	1,097.44
2020	0700	9/30/2020	BJBN0020	4000	4FA0	3RD QTR EP0 REIMBURSEMENT	2,460.00
2020	0700	9/30/2020	BJBN0020	4000	4FA1	3RD QTR EP0 REIMBURSEMENT	1,145.80
2020	0700	9/30/2020	BJBNEP22	1000	1306	4TH QTR EP0	1,661.66
2020	0700	9/30/2020	BJBNEP22	1000	1310	4TH QTR EP0	434.30
2020	0700	9/30/2020	BJBNEP22	1000	1320	4TH QTR EP0	1,069.74
2020	0700	9/30/2020	BJBNEP22	1000	1325	4TH QTR EP0	180.85
2020	0700	9/30/2020	BJBNEP22	2000	2100	4TH QTR EP0	850.10
2020	0700	9/30/2020	BJBNEP22	2000	2101	4TH QTR EP0	352.36
2020	0700	9/30/2020	BJBNEP22	2000	2102	4TH QTR EP0	726.10
2020	0700	9/30/2020	BJBNEP22	2000	2103	4TH QTR EP0	1,019.81

2020	0700	9/30/2020	BJBNEP22	2000	2113	4TH QTR EP0	1,384.21
2020	0700	9/30/2020	BJBNEP22	2000	2132	4TH QTR EP0	1,080.19
2020	0700	9/30/2020	BJBNEP22	2000	2134	4TH QTR EP0	627.18
2020	0700	9/30/2020	BJBNEP22	2000	2182	4TH QTR EP0	3,848.06
2020	0700	9/30/2020	BJBNEP22	2000	2313	4TH QTR EP0	704.50
2020	0700	9/30/2020	BJBNEP22	3000	3100	4TH QTR EP0	6,201.50
2020	0700	9/30/2020	BJBNEP22	3000	3111	4TH QTR EP0	624.47
2020	0700	9/30/2020	BJBNEP22	3000	3363	4TH QTR EP0	885.38
2020	0700	9/30/2020	BJBNEP22	4000	4100	4TH QTR EP0	3,770.14
2020	0700	9/30/2020	BJBNEP22	4000	4305	4TH QTR EP0	4,842.73
2020	0700	9/30/2020	BJBNEP22	4000	4402	4TH QTR EP0	484.82
2020	0700	9/30/2020	BJBNEP22	4000	4FA0	4TH QTR EP0	985.94
2020	0700	9/30/2020	BJBNEP22	4000	4FA1	4TH QTR EP0	1,275.68
2020	0700	9/30/2020	BJBNEP22	4000	4FA2	4TH QTR EP0	1,416.62
2020	0700	9/30/2020	BJBNEP32	1000	1040	4TH QTR EP0	2,376.01
2020	0700	9/30/2020	BJBNEP32	1000	1306	4TH QTR EP0	397.40
2020	0700	9/30/2020	BJBNEP32	1000	1310	4TH QTR EP0	1,308.72
2020	0700	9/30/2020	BJBNEP32	2000	2101	4TH QTR EP0	2,230.65
2020	0700	9/30/2020	BJBNEP32	2000	2103	4TH QTR EP0	1,633.16
2020	0700	9/30/2020	BJBNEP32	2000	2132	4TH QTR EP0	2,316.72
2020	0700	9/30/2020	BJBNEP32	2000	2133	4TH QTR EP0	777.85
2020	0700	9/30/2020	BJBNEP32	2000	2182	4TH QTR EP0	6,544.48
2020	0700	9/30/2020	BJBNEP32	2000	2308	4TH QTR EP0	913.83
2020	0700	9/30/2020	BJBNEP32	2000	2313	4TH QTR EP0	1,839.19
2020	0700	9/30/2020	BJBNEP32	3000	3100	4TH QTR EP0	3,148.34
2020	0700	9/30/2020	BJBNEP32	3000	3111	4TH QTR EP0	3,923.52
2020	0700	9/30/2020	BJBNEP32	3000	3363	4TH QTR EP0	1,145.79
2020	0700	9/30/2020	BJBNEP32	4000	4100	4TH QTR EP0	317.49
2020	0700	9/30/2020	BJBNEP32	4000	4305	4TH QTR EP0	5,111.06
2020	0700	9/30/2020	BJBNEP32	4000	4FA0	4TH QTR EP0	1,872.11
2020	0700	9/30/2020	BJBNEP32	4000	4FA1	4TH QTR EP0	704.72
2020	0700	9/30/2020	BJBNEP32	4000	4FA2	4TH QTR EP0	587.06
2020	0700	9/30/2020	BJBNOR20	3000	3100	COVID REIMBURSEMENT	851,109.52

						Final Budget	**$2,953,725.35**

PUBLIC SAFETY AND JUSTICE AGENCY							
FY 2021 REPROGRAMMING LIST							
LOCAL						**Starting Budget**	**$5,531,415.72**
FISCAL YEAR	**FUND**	**DATE**	**SOAR DOC #**	**Program**	**Activity**	**DESCRIPTION**	**AMOUNT**
2021	0100						$0.00
						Final Budget	**$5,531,415.72**

FEDERAL GRANT						**Starting Budget**	**$164,104,138.55**
FISCAL YEAR	**FUND**	**DATE**	**SOAR DOC #**	**Program**	**Activity**	**DESCRIPTION**	**AMOUNT**
2021	0200	10/1/2020	PABN0637	3000	3106	REPROGRAM FROM 4100F	$378,125.00
2021	0200	10/1/2020	PABN0637	3000	3109	REPROGRAM FROM 4100F	$665,000.00
2021	0200	10/1/2020	PABN0637	4000	4100	REPROGRAM TO 3106 AND 3109	($1,043,125.00)
2021	0200	10/8/2020	PABN0639	4000	4100	REPROGRAM FROM 013,015 & 050	$2,704,000.00
2021	0200	10/8/2020	PABN0639	4000	4100	REPROGRAM TO 0702	($2,704,000.00)
2021	0200	10/8/2020	PABN0644	2000	2113	REPROGRAM FROM 4100F & 5182F	$270,260.03
2021	0200	10/8/2020	PABN0644	2000	2308	REPROGRAM FROM 4100F & 5182F	$136,872.57
2021	0200	10/8/2020	PABN0644	3000	3109	REPROGRAM FROM 4100F & 5182F	$400,022.43
2021	0200	10/8/2020	PABN0644	3000	3111	REPROGRAM FROM 4100F & 5182F	$273,834.14

2021	0200	10/8/2020	PABN0644	3000	3116	REPROGRAM FROM 4100F & 5182F	$450,328.00
2021	0200	10/8/2020	PABN0644	4000	4100	REPROGRAM TO OTHER PCAS	($2,271,934.22)
2021	0200	10/8/2020	PABN0644	5000	5182	REPROGRAM FROM 4100F & 5182F	$1,023,736.43
2021	0200	10/8/2020	PABN0644	5000	5182	REPROGRAM TO OTHER PCAS	($589,159.38)
2021	0200	10/8/2020	PABN0644	5000	5183	REPROGRAM FROM 4100F & 5182F	$306,040.00
2021	0200	10/9/2020	PABN0645	1000	1309	REPROGRAM FROM OTHER PCAS	$113,449.66
2021	0200	10/9/2020	PABN0645	2000	2103	REPROGRAM FROM OTHER PCAS	$771,608.98
2021	0200	10/9/2020	PABN0645	2000	2103	REPROGRAM TO OTHER PCAS	($105,554.18)
2021	0200	10/9/2020	PABN0645	2000	2113	REPROGRAM FROM OTHER PCAS	$746,350.99
2021	0200	10/9/2020	PABN0645	2000	2113	REPROGRAM TO OTHER PCAS	($167,199.00)
2021	0200	10/9/2020	PABN0645	2000	2306	REPROGRAM FROM OTHER PCAS	$286,987.20
2021	0200	10/9/2020	PABN0645	2000	2308	REPROGRAM FROM OTHER PCAS	$36,121.97
2021	0200	10/9/2020	PABN0645	2000	2308	REPROGRAM TO OTHER PCAS	($8,837.00)
2021	0200	10/9/2020	PABN0645	3000	3111	REPROGRAM FROM OTHER PCAS	$247,605.55
2021	0200	10/9/2020	PABN0645	3000	3111	REPROGRAM TO OTHER PCAS	($15,000.00)
2021	0200	10/9/2020	PABN0645	3000	3113	REPROGRAM FROM OTHER PCAS	$348,702.55

2021	0200	10/9/2020	PABN0645	3000	3113	REPROGRAM TO OTHER PCAS	($103,657.00)
2021	0200	10/9/2020	PABN0645	3000	3363	REPROGRAM FROM OTHER PCAS	$17,149.47
2021	0200	10/9/2020	PABN0645	3000	3363	REPROGRAM TO OTHER PCAS	($500.00)
2021	0200	10/9/2020	PABN0645	3000	3402	REPROGRAM FROM OTHER PCAS	$250,000.00
2021	0200	10/9/2020	PABN0645	3000	3402	REPROGRAM TO OTHER PCAS	($246,302.43)
2021	0200	10/9/2020	PABN0645	4000	4100	REPROGRAM TO OTHER PCAS	($3,851,493.98)
2021	0200	10/9/2020	PABN0645	5000	5133	REPROGRAM FROM OTHER PCAS	$48,640.00
2021	0200	10/9/2020	PABN0645	5000	5133	REPROGRAM TO OTHER PCAS	($8,141.20)
2021	0200	10/9/2020	PABN0645	5000	5182	REPROGRAM FROM OTHER PCAS	$1,644,912.21
2021	0200	10/9/2020	PABN0645	5000	5183	REPROGRAM FROM OTHER PCAS	$77,482.21
2021	0200	10/9/2020	PABN0645	5000	5183	REPROGRAM TO OTHER PCAS	($82,326.00)
2021	0200	10/22/2020	PABN0650	2000	2113	REPROGRAM TO 4100F	($70,804.56)
2021	0200	10/22/2020	PABN0650	3000	3116	REPROGRAM TO 4100F	($167,807.00)
2021	0200	10/22/2020	PABN0650	4000	4100	REPROGRAM FROM 2113F & 3116F	$238,611.56
2021	0200	10/22/2020	PABN0651	4000	4100	REPROGRAM TO 5133 & 5182	($234,334.30)
2021	0200	10/22/2020	PABN0651	5000	5133	REPROGRAM FROM 4100, 5133,5182	$37,460.82
2021	0200	10/22/2020	PABN0651	5000	5182	REPROGRAM FROM 4100, 5133,5182	$334,334.30

2021	0200	10/22/2020	PABN0651	5000	5182	REPROGRAM TO 5133 & 5182	($100,000.00)
2021	0200	10/26/2020	BHBN0653	4000	4100	BUDGET ESTABLISHMENT	$65,000.00
2021	0200	10/26/2020	BHBN0654	4000	4100	BUDGET ESTABLISHMENT	$1,241,150.00
2021	0200	10/26/2020	BHBN0655	4000	4100	BUDGET ESTABLISHMENT	$1,999,141.00
2021	0200	11/4/2020	PABN0656	4000	4100	REPROGRAM FROM OTHER COBJ	$204,085.75
2021	0200	11/4/2020	PABN0656	4000	4305	REPROGRAM FROM OTHER COBJ	$199,632.00
2021	0200	11/4/2020	PABN0656	4000	4305	REPROGRAM TO OTHER COBJ	($403,717.75)
2021	0200	11/5/2020	PABN0657	4000	4100	REPROGRAM TO OTHER COBJ	($289,460.18)
2021	0200	11/5/2020	PABN0657	4000	4305	REPROGRAM FROM OTHER COBJ	$295,210.18
2021	0200	11/5/2020	PABN0657	4000	4305	REPROGRAM TO OTHER COBJ	($5,750.00)
2021	0200	11/5/2020	PABN0658	4000	4100	TO CORRECT ERROR	$0.00
2021	0200	11/6/2020	BHBN0659	2000	2100	BUDGET ESTABLISHMENT	$818,079.00
2021	0200	11/6/2020	BHBN0660	4000	4100	BUDGET ESTABLISHMENT	$150,000.00
2021	0200	11/17/2020	PABN0660	3000	3106	REPROGRAM FROM 4100F, 0506	$165,843.00
2021	0200	11/17/2020	PABN0660	4000	4100	REPROGRAM TO 3106, 0409	($165,843.00)
2021	0200	11/18/2020	PABN0651	5000	5133	REPROGRAM TO 5133 & 5182	($37,460.82)
2021	0200	12/16/2020	PABN0695	2000	2113	REPROGRAM FROM OTHER PCAS	$106,142.66

2021	0200	12/16/2020	PABN0695	2000	2308	REPROGRAM TO OTHER PCAS	($161,872.57)
2021	0200	12/16/2020	PABN0695	3000	3116	REPROGRAM FROM OTHER PCAS	$151,457.00
2021	0200	12/16/2020	PABN0695	4000	4100	REPROGRAM TO OTHER PCAS	($95,727.09)
2021	0200	12/16/2020	PABN0696	1000	1306	REPROGRAM FROM OTHER PCAS	$176,541.19
2021	0200	12/16/2020	PABN0696	1000	1306	REPROGRAM TO OTHER PCAS	($49,680.14)
2021	0200	12/16/2020	PABN0696	2000	2308	REPROGRAM TO OTHER PCAS	($46,812.00)
2021	0200	12/16/2020	PABN0696	4000	4100	REPROGRAM TO OTHER PCAS	($80,049.05)
2021	0200	1/7/2021	BHBN0697	4000	4100	BUDGET INCREASE	$104,260,626.99
2021	0200	1/11/2021	BHBN0698	2000	2100	BUDGET ESTABLISHMENT	$48,388.91
2021	0200	1/11/2021	BHBN0699	2000	2100	BUDGET ESTABLISHMENT	$1,184,958.84
2021	0200	1/11/2021	BHBN0700	2000	2100	BUDGET ESTABLISHMENT	$24,433.55
2021	0200	1/12/2021	BHBN0701	2000	2100	BUDGET ESTABLISHMENT	$67,414.47
						Final Budget	**$273,963,331.31**

Q14 HSEMA

Grant Year	Grant	Subrecipient	ID	Subaward	Amount	Awarded
2020	NSGP	Adas Israel Congregation	20NSGP891-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Alfred Street Baptist Church	20NSGP669-01	Nonprofit Security	90,000.00	10/13/2020
2020	NSGP	All Nations Baptist Church	20NSGP715-01	Nonprofit Security	85,671.00	10/13/2020
2020	NSGP	*Army Distaff Foundation*	20NSGP716-01	Nonprofit Security	47,512.00	10/13/2020
2020	NSGP	Brown Memorial AME Church	20NSGP717-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Calvary Baptist Church	20NSGP718-01	Nonprofit Security	59,000.00	10/13/2020
2020	NSGP	Charles E. Smith Jewish Day School	20NSGP561-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Chinese Community Church	20NSGP736-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Congregation B'nai Tzedek	20NSGP904-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Congregation Etz Hayim	20NSGP623-01	Nonprofit Security	64,000.00	10/13/2020
2020	NSGP	Congregation Olam Tikvah	20NSGP576-01	Nonprofit Security	69,500.00	10/13/2020
2020	NSGP	Emory Fellowship United Methodist Church	20NSGP733-01	Nonprofit Security	99,135.00	10/13/2020
2020	NSGP	Faith Tabernacle United Holy Church	20NSGP719-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Festival Center	20NSGP713-01	Nonprofit Security	91,854.00	10/13/2020
2020	NSGP	HIAS	20NSGP705-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Israel Baptist Church	20NSGP706-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Jewish Social Service Agency	20NSGP900-01	Nonprofit Security	67,375.00	10/13/2020
2020	NSGP	Kehilat Shalom	20NSGP653-01	Nonprofit Security	86,000.00	10/13/2020
2020	NSGP	Living Word International Christian Church	20NSGP720-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Miles Memorial Christian Methodist Episcopal Church	20NSGP707-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Mount Olive Baptist Church	20NSGP722-01	Nonprofit Security	95,200.00	10/13/2020
2020	NSGP	National City Christian Church	20NSGP723-01	Nonprofit Security	41,341.00	10/13/2020
2020	NSGP	National Community Church	20NSGP724-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	New Hope Freewill Baptist Church	20NSGP725-01	Nonprofit Security	75,000.00	10/13/2020
2020	NSGP	New Life Christian Church	20NSGP726-01	Nonprofit Security	85,500.00	10/13/2020
2020	NSGP	New York Avenue Presbyterian Church	20NSGP708-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Northern Virginia Hebrew Congregation	20NSGP709-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Peace Baptist Church	20NSGP694-01	Nonprofit Security	70,000.00	10/13/2020
2020	NSGP	Peoples Congregational United Church of Christ	20NSGP727-01	Nonprofit Security	76,000.00	10/13/2020
2020	NSGP	Pozez Jewish Community Center of Northern Virginia	20NSGP592-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Re'ese Adbarat Debre Selam Kidist Mariam	20NSGP728-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Revival Temple Church	20NSGP729-01	Nonprofit Security	91,650.00	10/13/2020
2020	NSGP	Rosemount Center	20NSGP710-01	Nonprofit Security	100,000.00	10/13/2020

2020	NSGP	Shiloh Baptist Church of Landover	20NSGP730-01	Nonprofit Security	89,575.00	10/13/2020
2020	NSGP	Sixth & I Historic Synagogue	20NSGP574-01	Nonprofit Security	91,991.00	10/13/2020
2020	NSGP	Southeast Hebrew Congregation	20NSGP555-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	St. Matthew's United Methodist Church	20NSGP731-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Stoddard Baptist Global Care	20NSGP711-01	Nonprofit Security	18,321.00	10/13/2020
2020	NSGP	Stoddard Baptist Home	20NSGP712-01	Nonprofit Security	21,279.00	10/13/2020
2020	NSGP	Temple Beth Ami	20NSGP698-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Temple B'nai Shalom	20NSGP732-01	Nonprofit Security	69,610.00	10/13/2020
2020	NSGP	Temple Solel	20NSGP657-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Washington Ethical Society	20NSGP734-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Washington National Cathedral	20NSGP667-01	Nonprofit Security	90,000.00	10/13/2020
2020	NSGP	Westminster Presbyterian Church	20NSGP714-01	Nonprofit Security	98,500.00	10/13/2020
2020	NSGP	Yad Yehuda of Greater Washington	20NSGP735-01	Nonprofit Security	100,000.00	10/13/2020
2020	NSGP	Yeshiva of Greater Washington	20NSGP577-01	Nonprofit Security	100,000.00	10/13/2020
2019	NSGP	Aish Greater Washington	19NSGP668-01	Nonprofit Security	84,800.00	10/23/2019
2019	NSGP	Alfred Street Baptist Church	19NSGP669-01	Nonprofit Security	95,497.00	10/23/2019
2019	NSGP	Al-Huda	19NSGP670-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Allen Chapel AME Church	19NSGP671-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Beth Chaverim Reform Congregation	19NSGP672-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	B'nai Shalom of Olney	19NSGP578-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Carolina Missionary Baptist Church	19NSGP674-01	Nonprofit Security	88,000.00	10/23/2019
2019	NSGP	Chabad at GW	19NSGP684-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Chabad Lubavitch of Alexandria-Arlington	19NSGP675-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Christ United Methodist Church	19NSGP676-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Church of the Epiphany	19NSGP699-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Congregation Beth Emeth	19NSGP704-01	Nonprofit Security	94,424.00	10/23/2019
2019	NSGP	Congregation Or Chadash	19NSGP677-01	Nonprofit Security	60,000.00	10/23/2019
2019	NSGP	Council on American-Islamic Relations (CAIR)	19NSGP673-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Dar Al-Hijrah Islamic Center	19NSGP678-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Empowerment Enterprise II	19NSGP679-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Fellowship Baptist Church	19NSGP680-01	Nonprofit Security	57,000.00	10/23/2019
2019	NSGP	Fifteenth Street Presbyterian Church	19NSGP681-01	Nonprofit Security	96,944.00	10/23/2019
2019	NSGP	Franconia United Methodist Church	19NSGP682-01	Nonprofit Security	60,200.00	10/23/2019
2019	NSGP	Greater Mount Calvary Holy Church	19NSGP683-01	Nonprofit Security	100,000.00	10/23/2019

2019	NSGP	Jewish Rockville Outreach Center	19NSGP612-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Jewish War Veterans of the USA	19NSGP685-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	John Wesley AME Zion Church	19NSGP687-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Kesher Israel Congregation	19NSGP624-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Maple Springs Baptist Church	19NSGP688-01	Nonprofit Security	75,752.00	10/23/2019
2019	NSGP	Maryland Jewish Experience (MEOR)	19NSGP700-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Matthews Memorial Baptist Church	19NSGP689-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Metropolitan AME Church	19NSGP690-01	Nonprofit Security	99,742.00	10/23/2019
2019	NSGP	New Samaritan Baptist Church	19NSGP691-01	Nonprofit Security	96,739.00	10/23/2019
2019	NSGP	Nineteenth Street Baptist Church	19NSGP692-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	North Chevy Chase Christian Church	19NSGP693-01	Nonprofit Security	68,836.00	10/23/2019
2019	NSGP	Ohev Sholom - The National Synagogue	19NSGP644-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Ohev Sholom Talmud Torah Congregation	19NSGP573-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Peace Baptist Church	19NSGP694-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Shepherd Park Christian Church	19NSGP695-01	Nonprofit Security	90,000.00	10/23/2019
2019	NSGP	Shiloh Baptist Church	19NSGP696-01	Nonprofit Security	95,000.00	10/23/2019
2019	NSGP	St. John's Church, Lafayette Square	19NSGP697-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Temple Beth Ami	19NSGP698-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Tifereth Israel Congregation	19NSGP902-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Unitarian Universalist Church of Arlington	19NSGP702-01	Nonprofit Security	99,411.00	10/23/2019
2019	NSGP	Washington National Cathedral	19NSGP667-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Woodside Synagogue Ahavas Torah	19NSGP639-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Yeshiva of Greater Washington	19NSGP577-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Young Israel Ezras Israel of Potomac	19NSGP640-01	Nonprofit Security	100,000.00	10/23/2019
2019	NSGP	Zion Baptist Church of Eastland Gardens	19NSGP703-01	Nonprofit Security	87,500.00	10/23/2019

Q15 HSEMA

Fiscal Year	Order ID	Contract ID	Supplier	Order Title	Amount	Contract Term	Competitively Bid	Contract Monitor	Monitoring Results	Funding Source
2020	PO611322	CW63677	TRAPWIRE INC.	FY2020- TrapWire System with User Licenses (8BNUA8)	$ 39,780.96	Date of award to 8/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO611421	N/A	Babel Street Inc.	FY2020- HSP/NTIC Situational Awareness Tool/Subscription (8BNUA8)	$ 37,500.00	Date of award to 9/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO611615	N/A	WASH METRO AREA TRANSIT A	FY2020- Administration/Facilities- Emergency bus contingency contract with WMATA	$ 7,000.00	Date of award to 9/30/2020	No	Robert Sneed	Satisfactorily	Local
2020	PO612056-V4	N/A	COMCAST BUSINESS COMMUNICATION	FY2020 - Administration/Facilities - Cable Transport Service and HDTV Service	$ 21,400.00	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Local
2020	PO612776-V2	N/A	GENERAL SERVICE ADMINISTRATION	FY2020- Administration/Facilities- Emergency Fleet Vehicles	$ 85,720.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Federal
2020	PO612953	C12805	MDM OFFICE SYSTEMS DBA	FY 2020- HSP/NTIC Secure Room Furniture/Technical Services (8BNUA8)	$ 10,000.00	Date of award to 9/30/2020	No	Whitney Bowen	Satisfactorily	Federal
2020	PO613881-V2	BPA-20-HSEMA-0003	NESTLE WATERS NORTH AMERICA	FY2020-Administration/Facilities- Emergency Water Supply	$ 15,000.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Federal
2020	PO614084	C12386	CAPITAL SERVICES AND SUPPLIES	FY 2020- BPA-Moving Services (including laborers, installers, drivers and equipment)	$ 8,000.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO614112	HGAC-RA05-18	MOTOROLA SOLUTIONS, INC.	FY2020- Admin/Facilities- Fleet Communication Package	$ 17,629.53	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO614124	C15484-V2	ALINEA PROMOS LLC	FY 2020- Operations- EOC- Deployment Polos	$ 9,915.25	Date of award to 9/30/2020	No	Donte Lucas	Satisfactorily	Federal
2020	PO614786-V2	BPA-20-HSEMA-0001	CAPITAL CITY RESTAURANT GROUP	FY 2020- Administration/Finance- Blanket Purchase Agreement for Catering	$ 11,755.00	Date of award to 9/30/2020	No	Briana Huggins	Satisfactorily	Federal
2020	PO615720	N/A	MICHAEL BAKER JR. INC.	FY 2020-HSP-LTRR/BCA Development (SMC17F)	$ 9,750.00	Date of award to 9/30/2020	No	Vermecia Alsop	Satisfactorily	Federal
2020	PO615757-V2	N/A	BEYONDTRUST CORPORATION	FY2020- Admin/IT Bomgar licenses (5BNUA9)	$ 10,473.75	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO616108	CW64233	SUPRETECH INC.	FY2020- Anti-malware software (5BNUA9)	$ 8,608.00	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO616292	C15842	SUPRETECH INC.	FY2020- Admin/IT Manage Engine Renewal (5BNUA9)	$ 17,158.20	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO616759	CW72776	EDGE360 LLC	FY2020- Administration IT- CCTV Software License Maint & Tech Support (5BNUA9)	$ 153,663.66	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO617224	N/A	RECOVERY POINT SYSTEMS INC.	FY2020- Administration/IT- Secure off-site backup data storage (5BNUA9)	$ 3,169.96	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO617230	CW74230	ADVANCED MEASUREMENT TECHNOLOG	FY 2020- Admin Grants- Type II RIIDs (STC17F)	$ 916,603.00	Date of award to 9/30/2020	Yes	Ingrid Naughton	Satisfactorily	Federal
2020	PO617232	N/A	GOTTA GO NOW LLC	FY2020-Administration/Facilities- Toilets, Portable, Rental or Lease, Mobile Command Cleaning/Sewage	$ 5,000.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO617237-V2	CW37689	ADVANCED EMPLOYEE INTELLIGENCE	FY2020 Professional Services Contract Support 6BNSH9 and DMC17F/17	$ 141,720.00	Date of award to 7/1/2020	Yes	Adriane Gill	Satisfactorily	Federal
2020	PO617279	C15484-V2	ALINEA PROMOS LLC	FY 2020- Operations- EOC- Deployment Polos and Cover up (15BNU8)	$ 9,997.40	Date of award to 9/30/2020	No	Donte Lucas	Satisfactorily	Federal
2020	PO617579	N/A	IDSI INTERNATIONAL INC.	FY 2020- JAHOC-Annual maintenance, hosting, updates and training (9BNUA9)	$ 32,000.00	Date of award to 9/30/2020	No	Frederick Goldsmith	Satisfactorily	Federal
2020	PO617675	N/A	GREAT AMERICAN CORP	FY2020 - Administration/Finance - Blanket Purchase Agreement for Catering	$ 10,000.00	Date of award to 9/30/2020	No	Briana Huggins	Satisfactorily	Federal
2020	PO617676	C12770-V3	METROPOLITAN OFFICE PRODUCTS	FY2020- Admin/Grants BPA Supplies (2018 M&A)	$ 5,000.00	Date of award to 9/30/2020	No	Charles Madden	Satisfactorily	Federal
2020	PO618023	N/A	XZOTECH SIGN AND DISPLAY LLC	FY2020- Professional signage BPA	$ 10,000.00	Date of award to 9/30/2020	No	Whitney Bowen	Satisfactorily	Local
2020	PO618268-V2	CW33909	MB STAFFING SERVICES LLC	Operation- FY 2020- Administrative Staff Support Emergency Operations Center	$ 129,879.00	Date of award to 12/31/2020	Yes	Robert Sneed	Satisfactorily	Local
2020	PO618425-V2	C12313	MB STAFFING SERVICES LLC	Operation- FY 2020-Jan 1 - March 31, 2020- Staffing Services Support JAHOC and Emergency Operations Center-Continuity Service	$ 50,000.00	Date of award to 3/31/2020	No	Robert Sneed	Satisfactorily	Local
2020	PO618439	N/A	COMCAST SPOTLIGHT	FY 2020- Office of the Director/OPA Ad Campaign (2BNSH8)	$ 75,000.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO618440	CW61753	AVAYA FEDERAL SOLUTIONS I	FY 2020- Admin/IT- Annual Telephone System Maintenance (5BNUA9)	$ 20,247.12	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO618446	CW73419	Bluebay Office Inc	FY2020- Exec/Ops- Blanket Purchase Agreement for Office Supplies	$ 7,000.00	Date of award to 9/30/2020	No	Monica Hill	Satisfactorily	Local
2020	PO618450-V2	CW64205	MERIDIAN KNOWLEDGE SOLUTIONS	FY2020-HSP-Planning, Training & Exercise-Learning Management Software Renewal (2BNUA9)	$ 47,000.00	Date of award to 9/30/2020	No	Jon Stewart	Satisfactorily	Federal
2020	PO618536	C16248	AL S OFFICE PRODUCTS	FY2020- Admin/Finance- Blanket Purchase Agreement for Office Supplies	$ 5,000.00	Date of award to 9/30/2020	No	Monica Hill	Satisfactorily	Local
2020	PO618622	C14322	BPM BI INC	FY2020- Admin IT Veritas Backup Exec License (5BNUA9)	$ 5,773.56	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO619549-V2	GS-03F-137DA	XEROX CORPORATION	FY2020- Administration/IT- Xerox Printer Annual Maintenance Renewal- GS-03F-137DA (5BNUA9)	$ 14,760.00	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO619571	N/A	JOHNSON CONTROLS SECURITY SOLU	FY2020 Admin/IT- Annual Alarm System	$ 8,580.88	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal

2020	PO619692	N/A	ANDRES MARQUEZ-LARA	FY 2020- Office of the Director-Senior Leadership Workshop Leadership Series	$ 4,000.00	Date of award to 9/30/2020	No	Jerica Shackelford	Satisfactorily	Local
2020	PO619739	C12770-V3	METROPOLITAN OFFICE PRODUCTS	FY2020- HSP/NTIC- Metropolitan Office Products- Blanket Purchase Agreement for Office Supplies (8BNUA8)	$ 5,000.00	Date of award to 9/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO619750-V2	CW42241	BANDB FLOOR SRVS DBA BANDB SOLUTIO	FY2020- Admin/Facilities Handyman services- B&B Solutions BPA #2	$ 2,500.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO619752-V2	N/A	MOTIR SERVICES INC	FY2020- Admin/Facilities Handyman services- Motir Services Inc BPA	$ 2,500.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO619967	CW77985	BUBBLE TECHNOLOGY INDUSTRIES	FY 2020 Admin Grants MDS- Helicopter, Maritime, Permanent (STC16F)	$ 758,850.00	Date of award to 9/30/2020	No	Ingrid Naughton	Satisfactorily	Federal
2020	PO620142	N/A	SPIN Global LLC	FY 2020-LTTR- Business Continuity Assessment Tool (SMC17F)	$ 8,000.00	Date of award to 9/30/2020	No	Vermecia Alsop	Satisfactorily	Federal
2020	PO620143	CW56205	ACTIVU CORPORATION	FY2020- Administration/IT- EOC Video Wall Maintenance (5BNUA9)	$ 90,709.29	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO620145-V2	GS-35F-253CA	ENVIRONMENTAL SYSTEMS RESEARCH	FY 2020-Directors Office- Dashboard (22BNU7) - GSA Contract GS-35F-253CA	$ 36,670.50	Date of award to 9/30/2020	No	Donte Lucas	Satisfactorily	Federal
2020	PO620468	N/A	SKYLINE NETWORK ENGINEERING LL	FY2020- Administration/IT- Firmware & Software(5BNUA9)	$ 39,686.40	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO620602	N/A	K2SHARE LLC	FY 2020- Administration Division/Grants- Annual License Renewal for SPARS (2018 UASI M&A)	$ 76,725.00	Date of award to 9/30/2020	No	Charles Madden	Satisfactorily	Federal
2020	PO620674	N/A	DC ARENA LIMITED PARTNERSHIP	FY 2020- Office of the Director/Digit LED board Adverstising (2BNSH9)	$ 45,000.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO620905	N/A	THE IMPACT GROUP LLC	FY2020- Admin/Facilities Dock forklift (15BNU7)	$ 33,186.09	Date of award to 9/30/2020	Yes	Kenneth Woodall	Satisfactorily	Federal
2020	PO621116	RK141834	COMLABS GOVERNMENT SYSTEMS	FY2020- Administration/IT- Emnet and Voice Manager Annual Renewal (5BNUA9)	$ 39,628.00	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO621316-V2	N/A	GLOBAL EQUIPMENT COMPANY INC	FY 2020- Operations/EOC Elevating Dock (15BNU8)	$ 9,079.33	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Federal
2020	PO621400	C15842	SUPRETECH INC.	FY 2020-IT/Admini Adobe Creative Cloud License & Indesign-(5BNUA9)	$ 5,524.04	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO621587	CW77836	MISSION CRITICAL PARTNERS, LLC	FY2020- Admin/IT- Technology Integrator for EOC and related Facilities (21BNU7)	$ 226,605.75	Date of award to 9/30/2020	No	Whitney Bowen	Satisfactorily	Federal
2020	PO621741	N/A	BALL AND BALL COMMUNICATION	FY2020 Admin/Facilities- BPA Response vehicle equipment installation	$ 10,000.00	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Local
2020	PO623131	DCAM-16-NC-0013D	RBK CONSTRUCTION AND DEVELOP	FY2020 Admin- Wall Repair and Painting BPA	$ 10,000.00	Date of award to 9/30/2020	No	Whitney Bowen	Satisfactorily	Local
2020	PO623481	N/A	PREDATA INC	FY2020- NTIC/NCRWatchDesk Foundation and Focus licenses (4BNUA8)	$ 38,400.00	Date of award to 9/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO623486	N/A	WILAND ASSOCIATES LLC	FY 2020- HSP/Preparedness- IMT Training Course- (14BNU9)	$ 210,544.00	Date of award to 9/30/2020	No	Jon Stewart	Satisfactorily	Federal
2020	PO623500	C1754-V3	SUPRETECH INC.	FY2020- IT- Windows 10 Licences - (7BNSH7)	$ 8,806.77	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO623595-V2	CW33909	MB STAFFING SERVICES LLC	Deobligate-FY 2020/Operations- Staffing Services Support JAHOC and Emergency Operations Center- Continunity II	$ 113,617.08	Date of award to 5/31/2020	Yes	Robert Sneed	Satisfactorily	Local
2020	PO623599	N/A	LAFAYETTE GROUP INC	FY2020 REPB/PTE- Communications Technician Training Course (2BNUA9)	$ 56,237.39	Date of award to 9/30/2020	No	Jon Stewart	Satisfactorily	Federal
2020	PO623864-V2	C12313	MB STAFFING SERVICES LLC	Operation- Staffing Services Support JAHOC and Emergency Operations Center (FY 2020-Jan 1 - March 31, 2020)	$ 148,324.00	Date of award to 3/31/2020	No	Robert Sneed	Satisfactorily	Local
2020	PO623936	N/A	IG LLC	FY2020 NTIC- Site Intelligence renewal 8BNUA9	$ 18,500.00	04/01/2020 - 09/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO623941-V2	C15336-V3	MVS INC	FY 2020- IT-VLA Office Pro Plus/Project Server License- (7BNSH7)	$ 84,165.80	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO623945	N/A	MARK EDWARD BRADY	FY 2020 -HSP- IMT Courses PIO & JIC Training- (2BNUA9)	$ 2,500.00	Date of award to 9/30/2020	No	Jon Stewart	Satisfactorily	Federal
2020	PO623946	N/A	PETER A. PIRINGER	FY 2020 -HSP- IMT Courses PIO & JIC Training Part 2 (2BNUA9)	$ 2,500.00	Date of award to 9/30/2020	No	Jon Stewart	Satisfactorily	Federal
2020	PO624182	C15336-V3	MVS INC	FY 2020- IT- Technical Supplies- (5BNUA9)	$ 8,410.17	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO624233	C15336-V3	MVS INC	FY 2020- Operations/EOC Software (8BNSH9)	$ 19,234.32	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO624241	C12770-V3	METROPOLITAN OFFICE PRODUCTS	FY2020 NTIC- Standing desks (8BNUA8)	$ 9,599.80	Date of award to 9/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO624680	N/A	METROPOLITAN OFFICE PRODUCTS	FY 2020- Operations/EOC Custom Cargo Trailer (15BNU8)	$ 10,046.40	Date of award to 9/30/2020	No	Kenneth Woodall	Satisfactorily	Federal
2020	PO625143	C14218-V2	EMERGENCY 911 SECURITY	FY 2020- IT-Cooling Solutions in Server Rooms- (7BNSH7)	$ 19,989.24	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO625144	C15484-V3	ALINEA PROMOS LLC	FY 2020- Executive Office- Agency Uniforms	$ 7,218.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO625210	C15842	SUPRETECH INC.	FY 2020- IT- ManageEngine Service Desk - (5BNUA9)	$ 5,476.80	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO625604	N/A	SHARP ELECTRONICS CORPORATION	FY 2020 - IT- Digital Signage System- (5BNUA9)	$ 21,451.00	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal

2020	PO625628-V2	N/A	EC AMERICA, INC.	FY2020 NTIC/Cyber- Authentic8 Silo Renewal (10BNU8) quote# QUO-1119654-N3X7R0	$ 8,448.80	Date of award to 9/30/2020	No	Krista Mazzeo	Satisfactorily	Federal
2020	PO626278	N/A	MVS INC	FY 2020 -IT- New Conference Room Reservation/Display System (7BNSH7)	$ 12,154.40	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO626382	N/A	COMCAST HOLDINGS CORPORATION	FY 2020/OPA-Hurricane Ad (2BNSH9)	$ 45,000.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO626633-V2	N/A	MB STAFFING SERVICES LLC	FY2020 Operations- Staffing Services Support JAHOC and Emergency Operations Center-Continuity III	$ 125,000.00	Date of award to 7/31/2020	No	Robert Sneed	Satisfactorily	Local
2020	PO626812-V2	C15994-V3	ABC TECHNICAL SOLUTIONS I	FY 2020- IT- EOC Refresh Dell Precision 3431 FF CTO- (7BNSH7)	$ 118,968.00	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO627847	C13842-V3	VERITAS CONSULTING GROUP	FY 2020- Executive Office- Security Camera Equipment and Installation	$ 9,942.00	Date of award to 9/30/2020	No	Whitney Bowen	Satisfactorily	Federal
2020	PO628177	N/A	ESI ACQUISITION	FY2020 Executive Office- WebEOC Support	$ 17,600.00	Date of award to 9/30/2020	No	Jerica Shackelford	Satisfactorily	Federal
2020	PO628191	N/A	BURTON ENTERPRISES LLC	FY2020-IT- Renewal of VOIP Service on Mobile Command Vehicle- (5BNUA9)	$ 14,337.60	Date of award to 9/30/2020	No	Timur Plavan	Satisfactorily	Federal
2020	PO628260	N/A	Articulate Global, Inc.	FY2020 REP/PTE- Articulate 360 (2BNUA9)	$ 6,170.25	Date of award to 9/30/2020	No	Jerica Shackelford	Satisfactorily	Federal
2020	PO628351	C15842	SUPRETECH INC.	FY 2020-Operations/EOC- Tablets Accessories (15BNU8)	$ 16,791.90	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO628357	N/A	PERPETUAL CORP	FY 2020/OPA-AlertDC Ad (2BNSH9)	$ 45,000.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO628367-V2	N/A	MB STAFFING SERVICES LLC	FY2020 Operations- Staffing Services Support JAHOC and Emergency Operations Center	$ 75,000.00	Date of award to 8/31/2020	No	Robert Sneed	Satisfactorily	Federal
2020	PO628470	N/A	OUTFRONT MEDIA INC.	2020/OPA-Print and Digital Advertising Placements (2BNSH9)	$ 19,392.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO628754-V3	N/A	MB STAFFING SERVICES LLC	FY2020 Operations- Staffing Services Support JAHOC and Emergency Operations Center	$ 80,000.00	Date of award to 9/30/2020	No	Robert Sneed	Satisfactorily	Local
2020	PO628755-V2	N/A	ESI ACQUISITION	FY 2020-Operations/EOC-Web based Support (8BNSH9)	$ 48,540.00	Date of award to 9/30/2020	No	Jerica Shackelford	Satisfactorily	Federal
2020	PO628757-V2	CW63677	TRAPWIRE INC.	Deobligate FY2020- TrapWire System with User Licenses (8BNUA9)	$ 3,731.45	Date of award to 9/30/2020	No	Madeline Marcenelle	Satisfactorily	Federal
2020	PO628759	C14281	SUPRETECH INC.	FY2020-IT-Dell Computers & Accessories-(7BNSH7)	$ 158,712.00	Date of award to 9/30/2020	Yes	Timur Plavan	Satisfactorily	Federal
2020	PO628904	N/A	WASHINGTON INFORMER NEWSPAPER	FY 2020/OPA-Hurricane Preparedness Campaign. (2BNSH9)	$ 8,800.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO629082	N/A	ALINEA PROMOS LLC	FY 2020- Operations-Agency Uniforms (15BNU8)	$ 6,282.30	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO629085-V2	N/A	WASHINGTON CITY PAPER	Deobligated-2020/OPA-Digital and Online Advertising(2BNSH9)	$ -	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO629459	N/A	HUBBARD RADIO WASHINGTON	FY 2020-OPA-ReadyDC campaign/Hurricane(2BNSH9)	$ 10,000.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO629837	N/A	MDE CITY PAPER HOLDINGS LLC	FY 2020/OPA-Digital and Online Advertising II (2BNSH9)	$ 10,320.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2020	PO629975	N/A	CRITICAL MENTION INC	FY 2020/OPA-Media Monitoring (2BNSH9)	$ 7,500.00	Date of award to 9/30/2020	No	Rebekah Mena	Satisfactorily	Federal
2021	PO630789-V3	PO	MB STAFFING SERVICES LLC	FY2021 Operations- Staffing Services Support JAHOC and Emergency Operations Center	$ 88,000.00	Date of award to 12/31/2020	No	Robert Sneed	(blank)	Local
2021	PO630860	N/A	COMCAST BUSINESS COMMUNICATION	FY2021 - Administration/Facilities - Cable Transport Service and HDTV Service	$ 21,400.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Local
2021	PO631027-V2	CW56205	ACTIVU CORPORATION	FY2021- Administration/IT- EOC Video Wall Maintenance (5BNUA9)	$ 94,739.04	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631086-V2	CW61753	AVAYA FEDERAL SOLUTIONS I	FY 2021- Admin/IT- Annual Telephone System Maintenance (5BNUA9)	$ 20,247.12	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631277	GS-03F-137DA	XEROX CORPORATION	FY2021- Administration/IT- Xerox Printer Annual Maintenance Renewal-(5BNUA9)	$ 14,760.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631638	N/A	ESI ACQUISITION	FY 2021-Operations/Interoperability - District Common Operating Pictures WebEOC System	$ 60,800.00	Date of award to 9/30/2021	No	Donte Lucas	(blank)	Federal
2021	PO631645	RK164608	SUPRETECH INC.	FY2021- Anti-malware software (5BNUA0)	$ 8,608.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631656-V2	RK164737	COMLABS GOVERNMENT SYSTEMS	FY2021- Administration/IT- Emnet and Voice Manager Annual Renewal (5BNUA0)	$ 41,418.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631735	N/A	RECOVERY POINT SYSTEMS INC.	FY2021- Administration/IT- Secure off-site backup data storage (5BNUA9)	$ 3,169.96	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO631913	N/A	SKYLINE NETWORK ENGINEERING LL	FY2021- Administration/IT- Firmware & Software(5BNUA9)	$ 39,686.40	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO632279	C15842	SUPRETECH INC.	FY2021- IT- Graphic Cards for EOC Computers- (7BNSH0)	$ 32,930.00	Date of award to 9/30/2021	Yes	Timur Plavan	(blank)	Federal
2021	PO632883	RK165577	WASH METRO AREA TRANSIT A	FY2021- Administration/Facilities- Emergency bus contingency contract with WMATA	$ 7,000.00	Date of award to 9/30/2021	No	Kenneth Woodall	(blank)	Local

2021	PO632884	RK165667	BALL AND BALL COMMUNICATION	FY 2021 Operations/Facilities- Response vehicle equipment installation	$ 10,000.00	Date of award 9/30/2021	No	Kenneth Woodall	(blank)	Local
2021	PO632949	GS-07F-225CA	JOHNSON CONTROLS SECURITY SOLU	FY2021 Admin/IT- SCIF and Fusion Center Security Annual Alarm System (5BNUA0)	$ 7,659.21	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO633379-V2	CW72776	EDGE360 LLC	FY2021- Administration IT- CCTV Software License Maint & Tech Support (5BNUA0)	$ 158,836.93	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO633640	N/A	GENERAL SERVICE ADMINISTRATION	FY2021- Operations/Facilities- Emergency Fleet Vehicles	$ 81,025.00	Date of award to 9/30/2021	No	Kenneth Woodall	(blank)	Local
2021	PO633942	N/A	Babel Street Inc.	FY2021- HSP/NTIC Situational Awareness Tool/Subscription (8BNUA9)	$ 31,250.00	Date of award to 9/30/2021	No	Madeline Marcenelle	(blank)	Federal
2021	PO633960	CW63677	TRAPWIRE INC.	FY2021- TrapWire System with User Licenses (8BNUA9)	$ 41,045.96	Date of award to 8/30/2021	No	Madeline Marcenelle	(blank)	Federal
2021	PO634312	N/A	CAPITAL CITY RESTAURANT GROUP	FY 2020-Mission Support- Catering Service	$ 3,500.00	Date of award to 9/30/2021	No	Briana Huggins	(blank)	Federal
2021	PO634409	N/A	BEYONDTRUST CORPORATION	FY2021- Admin/IT Bomgar licenses (5BNUA0)	$ 10,997.45	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO636023	CW85902	DIGI DOCS INC DOCUMENT MGERS	FY2021 Operations- Staffing Services Support JAHOC and Emergency Operations Center II	$ 217,530.00	Date of award to 9/30/2021	Yes	Robert Sneed	(blank)	Local
2021	PO636081	CW85900	THE COLES GROUP, LLC	FY2021 Operations- Staffing Services Support JAHOC and Emergency Operations Center I	$ 167,500.00	Date of award to 9/30/2021	Yes	Robert Sneed	(blank)	Local
2021	PO636099-V2	CW86579	MB STAFFING SERVICES LLC	FY2021 Operations- Staffing Services Support JAHOC and Emergency Operations Center Continuity	$ 10,000.00	Date of award to 12/31/2020	No	Robert Sneed	(blank)	Local
2021					$ 50,000.00	Date of award to 12/31/2020	No	Robert Sneed	(blank)	Local
2021	PO636280	N/A	CAPITAL CITY RESTAURANT GROUP	FY2021-Admin/Finance BPA for Catering	$ 10,000.00	Date of award to 9/30/2021	No	Briana Huggins	(blank)	Federal
2021	PO636281-V3	CW64205	MERIDIAN KNOWLEDGE SOLUTIONS	FY2021-HSP/PTE-Learning Management Software Renewal and Modification (2BNUA9/2BNUA0)	$ 77,000.00	Date of award to 9/20/2021	No	Jon Stewart	(blank)	Federal
2021	PO636641	CW77985	BUBBLE TECHNOLOGY INDUSTRIES	FY 2021 Admin Grants MDS- Helicopter, Maritime, Permanent (STC17F)	$ 758,850.00	Date of award to 9/30/2021	Yes	Ingrid Naughton	(blank)	Federal
2021	PO637027	N/A	OUTFRONT MEDIA INC.	FY2021- Executive Office/OPA- Inauguration Media Advertisement Services	$ 35,000.00	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021	PO637056	N/A	GEORGE WASHINGTON UNIVERSITY	FY 2021- Executive Office/COS-Leadership leadership coaching and workshops (2BNUA9)	$ 33,570.00	Date of award to 9/30/2021	No	Jerica Shackelford	(blank)	Federal
2021	PO637058	C12903-V2	METROPOLITAN OFFICE PRODUCTS	FY 2021- Executive Office/OPA- Inauguration Agency Uniforms	$ 35,767.43	Date of award to 9/30/2021	Yes	Rebekah Mena	(blank)	Federal
2021	PO637340	N/A	Zoho Corporation	FY 2021- IT- ManageEngine Renewal- (5BNUA0)	$ 16,426.80	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO637372-V2	N/A	ESI ACQUISITION	FY 2021-Operations/Interoperability - District Common Operating WebEOC System (6BNSH8)	$ 84,000.00	Date of award to 9/30/2021	No	Jerica Shackelford	(blank)	Federal
2021	PO637373-V2	CW86774	ANDEAN CONSULTING SOLUTIONS	FY2021- Executive Office/OPA- Inauguration Translation Services	$ 35,000.00	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021	PO637464	CW61043	NESTLE WATERS NORTH AMERICA	FY2021- Operations/Facilities- Inauguration Emergency Water Supply	$ 8,835.30	Date of award to 9/30/2021	No	Kenneth Woodall	(blank)	Federal
2021	PO637466	BPA-20-HSEMA-005	GOTTA GO NOW LLC	FY2021-Operations/Facilities- Toilets, Portable, Rental or Lease, Mobile Command Cleaning/Sewage	$ 5,000.00	Date of award to 9/30/2021	No	Kenneth Woodall	(blank)	Local
2021	PO637489	C17007	TPW CONSULTANTS LLC	FY 2021-Iridrium Postpaid Annual Service (5BNUA9)	$ 6,911.70	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO637701	N/A	IDSI INTERNATIONAL INC.	FY 2021- Operations/JAHOC-Annual maintenance, hosting, updates and training (9BNUA0)	$ 32,000.00	Date of award to 9/30/2021	No	Frederick Goldsmith	(blank)	Federal
2021	PO637874	N/A	JOHN WILEY AND SONS	FY 2021- Executive Office/COS- LPI 360 Assessment (2BNUA9)	$ 8,000.00	Date of award to 9/30/2021	No	Jerica Shackelford	(blank)	Federal
2021	PO637966	C16367-V6	TPW CONSULTANTS LLC	FY2021 IT-Additional Iridium Satellite Handset & Phone Services	$ 23,640.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO638004	C15842	SUPRETECH INC.	FY 2021- Executive Office/OPA- Inauguration JIC Supplies and Equipment	$ 5,232.51	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021	PO638005	GS-28F-0004X	MDM OFFICE SYSTEMS DBA	FY 2021- Executive Office/OPA- Inauguration JIC Chairs	$ 315.00	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021					$ 9,545.97	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021	PO638066	CW87531	ESRI-MID ATLANTIC USER GROUP	FY21- ArcGIS Platform (6BNSH8)	$ 297,620.00	Date of award to 9/30/2021	No	Donte Lucas	(blank)	Federal
2021	PO638179	C13809-V4	SENODA INC.	FY 2021- Executive Office/OPA- Inauguration Printing Services	$ 9,170.00	Date of award to 9/30/2021	No	Rebekah Mena	(blank)	Federal
2021	PO638412	CW77836	MISSION CRITICAL PARTNERS, LLC	FY2021-Office of Chief Staff - Professional Contract & Technical Services (MCP)- (16BNU8)	$ 70,000.00	Date of award 2/18/2021	No	Whitney Bowen	(blank)	Federal
2021	PO638425	N/A	THE DONOHOE COMPANIES INC	FY2021- Operations/Facilities- ADA Compliant Electric Door Openers	$ 3,925.00	Date of award to 9/30/2021	No	Kenneth Woodall	(blank)	Local
2021	PO638447	N/A	COBWEBS America INC	FY2021- NTIC Web Intelligence Platform (8BNUA0)	$ 98,000.00	Date of award to 9/30/2021	No	Madeline Marcenelle	(blank)	Federal

2021	PO638594	CW88797	ADVANCED MEASUREMENT TECHNOLOG	FY2021- Admin/Grants- Type I RIIDs (STC17)	$525,000.00	Date of award 9/30/2021	No	Ingrid Naughton	(blank)	Federal
2021	PO638602	N/A	WASH METRO AREA TRANSIT A	FY2021- Operations/JAHOC- Inauguration Emergency Incidents and Situations Buses	$ 10,000.00	Date of award to 9/30/2021	No	Robert Sneed	(blank)	Federal
2021	PO638608	N/A	CAPITAL CITY RESTAURANT GROUP	FY2021- Catering #2 (Inauguration)	$ 25,000.00	Date of award to 9/30/2021	No	Briana Huggins	(blank)	Federal
2021	PO638610	Contract # C000000614001 Customer Agreement # VA-190822-DELL	DELL MARKETING L.P.	FY2021- IT DCPIC laptops (Inauguration)	$ 37,215.80	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO638611	N/A	PINKE S E.A.T.S LLC	FY2021- Catering #3 (Inauguration)	$ 30,000.00	Date of award to 9/30/2021	No	Briana Huggins	(blank)	Federal
2021	PO638638	Contract # C000000614001 Customer Agreement # VA-190822-DELL	DELL MARKETING L.P.	FY2021- JIC monitors (Inauguration)	$ 8,270.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO638659	GSA# GS-03F-137DA SIN 333316C (purchase) and SIN 811212SA (maint)	XEROX CORPORATION	FY 2021- IT- Xerox Printers and Maintenance Services	$ 11,190.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021					$ 16,689.00	Date of award to 9/30/2021	No	Timur Plavan	(blank)	Federal
2021	PO638945	CW37689	ADVANCED EMPLOYEE INTELLIGENCE	FY 2021- Professional Services Contract Support	$ 2,500.00	Date of award to 7/1/2021	Yes	Adriane Gill	(blank)	Local
2021	PO638949	N/A	K2SHARE LLC	FY 2021- Admin/Grants- Renewal of Grant Management System-	$ 76,725.00	Date of award to 9/30/2021	No	Charles Madden	(blank)	Federal
2021	PO639096	N/A	THERMO FISHER SCIENTIFIC, LLC	FY2021- Admin/Grants- Survey Kits (STC17)	$ 71,523.20	Date of award to 9/30/2021	No	Ingrid Naughton	(blank)	Federal

Homeland Security and Emergency Management Agency FY2020

Agency Homeland Security and Emergency Management Agency **Agency Code** BN0 **Fiscal Year** 2020

Mission The Mission of the District of Columbia Homeland Security and Emergency Management Agency (HSEMA) is to lead the planning and coordination of homeland security and emergency management efforts to ensure that the District of Columbia is prepared to prevent, protect against, respond to, mitigate, and recover from all threats and hazards.

Summary of Services HSEMA plans and prepares for emergencies; coordinates emergency response and recovery efforts; provides training and conducts exercises for emergency first responders, employees and the public; provides emergency preparedness information to the public; and disseminates emergency information.

2020 Accomplishments

Accomplishment	Impact on Agency	Impact on Residents
In 2018, HSEMA in coordination with the EPC, established Disaster Logistics as one of seven strategic priorities for the District's preparedness program. The District's response to the COVID-19 pandemic required demonstration and rapid expansion of this capability to meet the needs of the District's residents and government agencies. In response, HSEMA – working with OCP, DPW, and DCNG – operationalized a new warehouse, the Disaster Logistics Center (DLC), to store, manage, and distribute disaster supplies including personal protective equipment, water, and surge mass care equipment. Additionally, HSEMA expanded the District's resource management capability through expansion of the EOC's Resource Unit and refinement of resource management processes in WebEOC.	While expansion of HSEMA's logistics capability marks a notable development in our ability to support our partner agencies during COVID response and in future disasters, it does require a significant and sustained resource investment, specifically in the form of staff now dedicated to management and operation of the DLC.	The DLC houses critical emergency supplies which the District now has on hand for rapid deployment to residents or to other District agencies to support delivery of their services in the community. Having these resources on hand, and the systems in place to manage and distribute them, reduces the time it takes to meet the vital needs of the District's residents in response to future emergencies or disasters.
In early March, with minimal notice, HSEMA was able to relocate EOC operations and the Joint Information Center (JIC) to the Health Emergency Coordination Center to collocate with DC Health during COVID-19 response. This demonstrated HSEMA's ability to operationalize its COOP plans at a new location quickly and with minimal disruption to operations. HSEMA maintained this COOP posture for 7.5 months while building capability and capacity to operate a virtual EOC should future emergencies require virtual operations.	Establishing and operationalizing both COOP and virtual EOC operations demonstrated operational capability and resiliency while offering an opportunity for training HSEMA staff, emergency liaison officers and public information officers from partner agencies on non-standard EOC and response operations.	Capacity built and demonstrated through these operations ensures the EOC is resilient and operational in the face of both standard emergencies and large-scale disasters, allowing for rapid response and resource coordination to meet the immediate needs of residents in an emergency.
In addition to staffing and managing the EOC/JIC/HECC for COVID-19 response, HSEMA staff members were embedded in all aspects of the response operations providing long-term staff support to the Health and Medical, Human Services, Fatality Management, and Education Branches as well as the Mission Support and Government Operations Sections. HSEMA staff also led and staffed the Recovery Section and served as Incident Commander, Planning Section Chief, and Deputy Operations Chief for the District's Incident Management Team. Additionally, HSEMA staff played an integral role in the JIC mission of communicating timely, accurate, and accessible information to the public. During COVID response, HSEMA also supported response to multiple concurrent incidents including Hurricane Isaias, First Amendment events in June, the August March on Washington, the September 10th flooding event, and heat emergencies throughout the summer months. Prior to COVID response, the EOC was activated for five days in support of events associated with the Nationals' World Series victory.	Capacity built and demonstrated through these operations validates two years of interim process improvements and ensures the EOC and JIC are resilient and operational in the face of both standard emergencies and large-scale disasters. This allows for rapid response and resource coordination to meet the immediate needs of residents in an emergency. However, sustained response operations required staff to work extended hours in their operational roles significantly reducing available bandwidth for execution of steady state priorities and operations.	The demonstrated ability of the EOC to stretch for a months long COVID response while simultaneously surging to meet the needs of concurrent events and emergencies ensured that residents had ready access to emergency information and resources throughout the year. Additionally, by establishing the EOC and JIC early in the COVID response, the District – coordinated by HSEMA – established critical response elements including (1) a city-wide testing program at fixed sites and rotating locations; (2) expanded social services support through grocery and meal delivery; (3) expanded mortuary capacity; (4) a 428 bed alternate care facility; (5) on-demand family assistance for every family that lost a loved one to COVID, and (6) translated critical life-saving information for residents into the District's six required languages.

2020 Key Performance Indicators

Measure	Frequency	FY 2017 Actual	FY 2018 Actual	FY 2019 Actual	FY 2020 Target	FY 2020 Quarter 1	FY 2020 Quarter 2	FY 2020 Quarter 3	FY 2020 Quarter 4	FY 2020 Actual	KPI Status	Explanation for Unmet FY 2020 Target
1 - Emergency Operations – Provide situational awareness, logistical and resource support, and a field command operation to coordinate critical incident response, mitigation, and recovery to emergencies and other major events impacting the District of Columbia. (3 Measures)												
Percent of employees with activation responsibilities qualified in their EOC role	Quarterly	New in 2020	New in 2020	New in 2020	New in 2020	100%	100%	100%	100%	100%	New in 2020	
Percentage of eligible EOC staff in attendance at EOC Readiness training per quarter	Quarterly	New in 2020	New in 2020	New in 2020	New in 2020	No applicable incidents	No applicable incidents	No applicable incidents	No applicable incidents	No applicable incidents	New in 2020	
Percentage of weekly EOC facility inspections completed per quarter	Quarterly	New in 2020	New in 2020	New in 2020	New in 2020	100%	100%	100%	No applicable incidents	100%	New in 2020	
2 - Intelligence and Analysis – Improve information sharing among public and private sector partners by providing strategic analysis of regional threats and hazards. (2 Measures)												
Percent of distributable analytic products co-authored with one or more federal, state or local partners	Quarterly	39.4%	11.4%	2.9%	10%	4.3%	25%	2.6%	5.3%	5.1%	Unmet	As an all-hazards fusion center many of the NTIC resources were leveraged towards the COIVD-19 response this FY. This type of production does not lend itself to joint sealed production, as it is specific to the NTIC's AOR.

Measure	Frequency	FY 2017 Actual	FY 2018 Actual	FY 2019 Actual	FY 2020 Target	FY 2020 Quarter 1	FY 2020 Quarter 2	FY 2020 Quarter 3	FY 2020 Quarter 4	FY 2020 Actual	KPI Status	Explanation for Unmet FY 2020 Target
Percent of increase in the number of subscribers to fusion center situational and analytic product distribution lists	Quarterly	14.8%	10.4%	11.7%	10%	2%	2.8%	2.5%	-71.3%	-69.1%	Unmet	During FY20 Q4 the NTIC scrubbed its distribution list and required all recipients remaining on the list to sign a new non-disclosure agreement (NDA) to continue receiving products. This resulted in the removal of approximately 3,000 legacy recipients, mostly from inactive email addresses, etc.
3 - Ready DC – Ready DC is a comprehensive approach to building capabilities related to homeland security and emergency management. It includes the personnel, processes, plans, and resources necessary to build each preparedness capability to target levels. Once built, these capabilities enable the District to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that affect the city. (3 Measures)												
Percent of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements	Annually	95.9%	83.3%	92.6%	95%	Annual Measure	Annual Measure	Annual Measure	Annual Measure	92.59%	Nearly Met	Though the majority of staff have completed their training, staff turnover and limited bandwidth for training during COVID response were limiting factors in meeting this target.
Percent of EMAP accreditation standards for which HSEMA has current documentation	Annually	New in 2020	New in 2020	New in 2020	New in 2020	Annual Measure	Annual Measure	Annual Measure	Annual Measure	81.25%	New in 2020	
Percentage of new or revised plans (where the planning process was led by HSEMA) socialized through training or exercise.	Annually	New in 2020	New in 2020	New in 2020	New in 2020	Annual Measure	Annual Measure	Annual Measure	Annual Measure	4.44%	New in 2020	
4 - Agency Management – Ensure that HSEMA provides its divisions with sufficient resources while ensuring that all fiscal requirements are fulfilled. (3 Measures)												
Percent of federal subgrants issued within 45 days of award receipt	Annually	93.5%	99.3%	90.8%	90%	Annual Measure	Annual Measure	Annual Measure	Annual Measure	88.51%	Nearly Met	The 45-day pass through deadline is in October after the end of the Q4 reporting period; final results can be reported after the 45 window has closed.
Percent of grant dollars spent within the timeframe of the grants	Annually	80.5%	97.8%	98.3%	98%	Annual Measure	Annual Measure	Annual Measure	Annual Measure	99.79%	Met	
Percent increase in the number of recipients of AlertDC	Quarterly	3.9%	9.9%	3%	3%	3.6%	3.3%	22.8%	4.6%	40.1%	Met	

2020 Workload Measures

Measure	FY 2018 Actual	FY 2019 Actual	FY 2020 Quarter 1	FY 2020 Quarter 2	FY 2020 Quarter 3	FY 2020 Quarter 4	FY 2020 PAR
1 - Deploy HSEMA personnel through EMAC in support of emergency or special event operations in other jurisdictions (1 Measure)							
Number of days agency staff are deployed out of District to support response and recovery activities in other jurisdictions	New in 2020	New in 2020	Annual Measure	Annual Measure	Annual Measure	Annual Measure	0
1 - Emergency Operations Center (EOC) (6 Measures)							
Number of level 3 (enhanced) or higher Emergency Operations Center activations	5	4	7	2	2	2	13
Number of days JAHOC teams are deployed to special events	New in 2020	New in 2020	9	1	0	2	12
Number of AlertDC messages sent to the public	New in 2020	New in 2020	2242	2380	2469	2580	9671
Number of HSEMA alerts sent to District government staff	New in 2020	New in 2020	10	996	1530	1465	4001

Measure	FY 2018 Actual	FY 2019 Actual	FY 2020 Quarter 1	FY 2020 Quarter 2	FY 2020 Quarter 3	FY 2020 Quarter 4	FY 2020 PAR
Number of days agency staff are deployed to incident sites	New in 2020	New in 2020	8	22	71	66	167
Alerts processed through JAHOC inbox	New in 2020	New in 2020	2670	2402	2376	2281	9729
2 - Tactical Analysis (2 Measures)							
Number of raw suspicious activity reports (SARs) processed	448	440	126	140	106	93	465
Number of requests for information (RFIs) processed	672	437	101	103	129	116	449
3 - Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities (1 Measure)							
Number of District plans created, revised, or reviewed for District Government partners annually	155	100	43	14	0	41	98
3 - Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities (4 Measures)							
Number of trainings provided to first responders, District employees, and the public by HSEMA	55	130	7	18	0	1	26
Number of individuals trained by HSEMA	1007	1591	324	310	0	63	697
Number of executive level staff completing an emergency senior/cabinet level training within 60 days of onboarding	1	0	0	1	0	0	1
Percent of District agencies with lead and support roles that participated in HSEMA led trainings or exercises	34.1%	85.2%	20.1%	14%	No applicable incidents	1.3%	11.8%
4 - Community Outreach & Media Prepare (1 Measure)							
Number of community outreach events attended or conducted by HSEMA	205	234	47	35	0	7	89
4 - Mayor's Special Event Task Group (MSETG) (1 Measure)							
Number of special events that have been processed by the Mayor's Special Events Task Group	116	92	12	30	6	0	48
4 - Serves as the State Administrative Agent for the federal homeland security grant programs that are awarded to the District of Columbia, and the National Capital Region (NCR) (3 Measures)							
Number of reimbursements processed for subrecipients annually	4025	3579	Annual Measure	Annual Measure	Annual Measure	Annual Measure	3227
Number of active subawards	New in 2020	New in 2020	384	336	346	253	1319
Number of grant monitoring visits	New in 2020	New in 2020	0	0	0	0	0

2020 Operations

Operations Header	Operations Title	Operations Description	Type of Operations
1 - Emergency Operations – Provide situational awareness, logistical and resource support, and a field command operation to coordinate critical incident response, mitigation, and recovery to emergencies and other major events impacting the District of Columbia. (2 Activities)			
Emergency Operations Center (EOC)	Emergency Operations Center (EOC)	- Manage the EOC, a central facility for command and control of emergency operations, which coordinates interagency response to and recovery from major emergencies and works closely with supporting District agencies before and during EOC activations. On a daily basis, the JAHOC serves this function as the 24/7 central hub of communications, processing information from multiple sources to keep District agencies, regional and Federal partners, businesses, and the public informed and create a common operating picture.	Daily Service
Emergency Management Assistance Compact (EMAC)	Deploy HSEMA personnel through EMAC in support of emergency or special event operations in other jurisdictions	HSEMA emergency operations center personnel deploy to other states and localities to assist with emergency response or special events.	Daily Service
2 - Intelligence and Analysis – Improve information sharing among public and private sector partners by providing strategic analysis of regional threats and hazards. (3 Activities)			
Information Sharing	Information Sharing	Ensure timely, relevant, and vetted intelligence information and analysis related to the safety and security of District citizens and first responders is provided to local, regional, and national public safety partners.	Daily Service
STRATEGIC ANALYSIS	Strategic Analysis	Provide strategic analysis and assessments of threats and hazards for public safety partners and decision makers by researching, analyzing, and synthesizing regional patterns and trends.	Daily Service
Tactical Analysis	Tactical Analysis	Provide tactical intelligence support and open source research, both in response to requests as well as on an ad hoc basis, to public and private sector partners in the public safety community in a timely manner.	Daily Service
3 - Ready DC – Ready DC is a comprehensive approach to building capabilities related to homeland security and emergency management. It includes the personnel, processes, plans, and resources necessary to build each preparedness capability to target levels. Once built, these capabilities enable the District to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that affect the city. (5 Activities)			
Capability Building	Capability Building	Identify and implement projects to build priority preparedness capabilities to target levels.	Daily Service
UASI Funding	UASI Funding	Continue to drive the District's competitiveness in receiving Urban Area Security Initiative (UASI) grant funds by ensuring District priorities are represented in regional strategies, and identifying projects to move priority regional capabilities towards target levels.	Daily Service
Continuity of Operations (COOP) Planning	Continuity Of Operations (COOP) Planning	Support the District agencies responsible for updating their COOP plans annually with exercising, evaluating, and, if necessary, revising their COOP plans.	Daily Service

Operations Header	Operations Title	Operations Description	Type of Operations
PLANNING	Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities	Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities.	Daily Service
TRAINING	Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities	Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities.	Daily Service
4 - Agency Management – Ensure that HSEMA provides its divisions with sufficient resources while ensuring that all fiscal requirements are fulfilled. (4 Activities)			
Regional Support	Regional Support	Provides leadership to the NCR as members of regional homeland security and emergency management leadership teams and supporting governance groups.	Daily Service
COMMUNITY OUTREACH & MEDIA PREPARE	Community Outreach & Media Prepare	Maintain a strong outreach program designed to educate and equip community residents and businesses to prepare for and recover from all hazards and the potential for disasters.	Daily Service
Grants Management	Serves as the State Administrative Agent for the federal homeland security grant programs that are awarded to the District of Columbia, and the National Capital Region (NCR)	Provides financial and programmatic oversight to various grant programs administered by DC HSEMA including emergency preparedness and response and recovery programs. Administers numerous individual subawards/projects in the District of Columbia and the National Capital Region.	Daily Service
Mayor's Special Event Task Group (MSETG)	Mayor's Special Event Task Group (MSETG)	Manage the administration of the MSETG, a body responsible for organizing the City's public safety planning efforts for events requiring interagency coordination.	Daily Service

2020 Strategic Initiatives

Strategic Initiative Title	Strategic Initiative Description	Completion to Date	Status Update	Explanation for Incomplete Initiative
Capability Building (1 Strategic Initiative)				
Watts Branch Home Surveys	In FY20, HSEMA will complete home surveys in Watts Branch (Ward 7) to determine the eligibility of homes for floodproofing mitigation. These surveys will be used to create a FloodSmart program, similar to RiverSmart and Great Streets, and increase the resilience of the community against potential flooding impacts.	Complete	The results from the original survey were used to compile the Executive Summary – FloodSmart Home Research for communities in Wards 6, 7 and 8. The attached report outlines the path forward to develop new flood mitigation projects using a long-term strategy to implement the FloodSmart Program by completing residential flood retrofits. Refer to the attached Executive Summary.	
Community Outreach & Media Prepare (1 Strategic Initiative)				
Community Insurance Trainings	In FY20, HSEMA will create an outreach workshop in Ward 8 focused on insurance coverage including home owner, rental, and commercial policies. The workshops will also cover how FEMA and the Small Business Administration may subsidize insurance after a disaster or major loss.	Complete	Conducted Flood Insurance Stakeholder Workshop, producing preliminary approaches for improving community outreach. Engaged contractor services to implement outreach in Ward 8 along Watts Branch	
Emergency Operations Center (EOC) (1 Strategic Initiative)				
Emergency Operations Center Renovations	In FY20, HSEMA will continue to upgrade the capabilities of the District's Emergency Operations Center (EOC). Working with the Department of General Services, HSEMA will redesign the EOC floor space to increase efficiency and maximize capacity during operations. HSEMA expects the design phase of this project to be complete by the end of FY20. In addition, HSEMA expects to have an enhanced situational awareness platform in place by the close of FY20.	25-49%	To date, HSEMA and the DGS A/E contractor have worked to create a final set of design concepts. Drawings and schematics will begin in November 2020.	The initial design required amendment to accommodate adjusted requirements. Funding intended to support these changes was unavailable due to COVID. Design adjustments will recommence in November with anticipated completion in March 2021.
Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities (1 Strategic Initiative)				
IMT Academy	In FY20, HSEMA will lead the inter-agency Incident Management Team Academy, which will graduate its first cohort and welcome a second cohort. Each IMT cohorts will provide enhanced incident management and emergency preparedness capabilities to District agencies and partners, building combined strength across the District for the management of major incidents.	50-74%	Our ability to deliver classes and conduct exercises are on hold indefinitely through COVID-19. We have reset our completion target for the first cohort to the end of 2021 so that we can potentially use the District's 2021 Inauguration and planning as part of our cohort opportunities for evaluation of skills.	Our ability to deliver classes and conduct exercises are on hold indefinitely through COVID-19. We have reset our completion target for the first cohort to the end of 2021 so that we can potentially use the District's 2021 Inauguration and planning as part of our cohort opportunities for evaluation of skills.
Strategic Analysis (1 Strategic Initiative)				
Physical Risk Assessment Teams	In FY20, HSEMA will establish physical risk assessment teams to conduct periodic physical risk assessments of District government buildings to identify vulnerabilities that could put the facilities at increased risk. Teams will be formed, trained, and ready for deployment by the end of FY20	0-24%	Due to high staff turnover and tasking of new staff to training/onboarding and preparation for the presidential election and inauguration no work has been done this quarter. Additionally, trainings are postponed in light of COVID-19.	Due to high staff turnover and tasking of new staff to training/onboarding and preparation for the presidential election and inauguration no work has been done this quarter. Additionally, trainings are postponed in light of COVID-19.

Homeland Security and Emergency Management Agency FY2021

Agency Homeland Security and Emergency Management Agency **Agency Code** BN0 **Fiscal Year** 2021

Mission The Mission of the District of Columbia Homeland Security and Emergency Management Agency (HSEMA) is to lead the planning and coordination of homeland security and emergency management efforts to ensure that the District of Columbia is prepared to prevent, protect against, respond to, mitigate, and recover from all threats and hazards.

Strategic Objectives

Objective Number	Strategic Objective
1	Emergency Operations – Provide situational awareness, logistical and resource support, and a field command operation to coordinate critical incident response, mitigation, and recovery to emergencies and other major events impacting the District of Columbia.
2	Homeland Security and Intelligence – Improve information sharing among public and private sector partners by providing strategic analysis of regional threats and hazards.
3	Resilience and Emergency Preparedness – Resilience and Emergency Preparedness is a comprehensive approach to building capabilities related to homeland security and emergency management. It includes the personnel, processes, plans, and resources necessary to build each preparedness capability to target levels. Once built, these capabilities enable the District to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that affect the city.
4	Agency Management – Ensure that HSEMA provides its divisions with sufficient resources while ensuring that all fiscal requirements are fulfilled.
5	Create and maintain a highly efficient, transparent, and responsive District government.

Key Performance Indicators

Measure	Directionality	FY 2018 Actual	FY 2019 Actual	FY 2020 Actual	FY 2021 Target
1 - Emergency Operations – Provide situational awareness, logistical and resource support, and a field command operation to coordinate critical incident response, mitigation, and recovery to emergencies and other major events impacting the District of Columbia. (3 Measures)					
Percent of employees with activation responsibilities trained in their EOC role	Up is Better	New in 2020	New in 2020	100%	90%
Percentage of eligible EOC staff in attendance at EOC Readiness training per quarter	Up is Better	New in 2020	New in 2020	No Applicable Incidents	90%
Percentage of weekly EOC facility inspections completed per quarter	Up is Better	New in 2020	New in 2020	100%	100%
2 - Homeland Security and Intelligence – Improve information sharing among public and private sector partners by providing strategic analysis of regional threats and hazards. (2 Measures)					
Percent of distributable analytic products co-authored with one or more federal, state or local partners	Up is Better	11.4%	2.9%	5.1%	10%
Percent of increase in the number of subscribers to fusion center situational and analytic product distribution lists	Up is Better	10.4	11.7	-71.3	10
3 - Resilience and Emergency Preparedness – Resilience and Emergency Preparedness is a comprehensive approach to building capabilities related to homeland security and emergency management. It includes the personnel, processes, plans, and resources necessary to build each preparedness capability to target levels. Once built, these capabilities enable the District to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that affect the city. (7 Measures)					
Percent of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements	Up is Better	83.3%	92.6%	92.6%	95%
Percent of EMAP accreditation standards for which HSEMA has current documentation	Up is Better	New in 2020	New in 2020	81.3%	95%
Percentage of new or revised plans (where the planning process was led by HSEMA) socialized through training, exercise, or real-world events.	Up is Better	New in 2020	New in 2020	4.4%	90%
Percentage of executive level staff with responsibilities in the Emergency Operations Plan completing an emergency senior/cabinet level training within 60 days of onboarding	Up is Better	New in 2021	New in 2021	New in 2021	New in 2021
Percent of District agencies with lead and support roles in the District Preparedness Framework that participated in HSEMA led trainings or exercises	Up is Better	New in 2021	New in 2021	New in 2021	New in 2021
Amount of competitive grant funding awarded to HSEMA for resilience and hazard mitigation	Up is Better	New in 2021	New in 2021	New in 2021	New in 2021
Percentage of Single Member Districts where HSEMA conducted a community preparedness training or event.	Up is Better	New in 2021	New in 2021	New in 2021	New in 2021
4 - Agency Management – Ensure that HSEMA provides its divisions with sufficient resources while ensuring that all fiscal requirements are fulfilled. (3 Measures)					
Percent of federal subgrants issued within 45 days of award receipt	Up is Better	99.3%	90.8%	88.5%	90%
Percent of grant dollars spent within the timeframe of the grants	Up is Better	97.8%	98.3%	99.8%	98%
Percent increase in the number of recipients of AlertDC	Up is Better	9.9%	3%	40.1%	3%

Operations

Operations Header	Operations Title	Operations Description	Type of Operations
1 - Emergency Operations – Provide situational awareness, logistical and resource support, and a field command operation to coordinate critical incident response, mitigation, and recovery to emergencies and other major events impacting the District of Columbia. (3 Activities)			
Emergency Operations Center (EOC)	Emergency Operations Center (EOC)	- Manage the EOC, a central facility for command and control of emergency operations, which coordinates interagency response to and recovery from major emergencies and works closely with supporting District agencies before and during EOC activations. On	Daily Service
Incident Management	Deployment for incident managment	Deploy HSEMA personnel across the District to manage incidents, and to other jurisdictions to support incident response and management through EMAC.	Daily Service
Logistics Management	Manage Disaster Logistics Center	Manage the District's Disaster Logistics Center warehouse and coordinate disaster logistics operations during incident response.	Daily Service
2 - Homeland Security and Intelligence – Improve information sharing among public and private sector partners by providing strategic analysis of regional threats and hazards. (3 Activities)			
Tactical Analysis	Tactical Analysis	Provide tactical intelligence support and open source research, both in response to requests as well as on an ad hoc basis, to public and private sector partners in the public safety community in a timely manner.	Daily Service
STRATEGIC ANALYSIS	Strategic Analysis	Provide strategic analysis and assessments of threats and hazards for public safety partners and decision makers by researching, analyzing, and synthesizing regional patterns and trends.	Daily Service
Information Sharing	Information Sharing	Ensure timely, relevant, and vetted intelligence information and analysis related to the safety and security of District citizens and first responders is provided to local, regional, and national public safety partners.	Daily Service
3 - Resilience and Emergency Preparedness – Resilience and Emergency Preparedness is a comprehensive approach to building capabilities related to homeland security and emergency management. It includes the personnel, processes, plans, and resources necessary to build each preparedness capability to target levels. Once built, these capabilities enable the District to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that affect the city. (5 Activities)			
UASI Funding	UASI Funding	Continue to drive the District's competitiveness in receiving Urban Area Security Initiative (UASI) grant funds by ensuring District priorities are represented in regional strategies, and identifying projects to move priority regional capabilities towards target levels.	Daily Service
Continuity of Operations (COOP) Planning	Continuity Of Operations (COOP) Planning	Support the District agencies responsible for updating their COOP plans annually with exercising, evaluating, and, if necessary, revising their COOP plans.	Daily Service
Capability Building	Capability Building	Identify and implement projects to build priority preparedness capabilities to target levels.	Daily Service
PLANNING	Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities	Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities.	Daily Service
TRAINING	Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities	Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities.	Daily Service
4 - Agency Management – Ensure that HSEMA provides its divisions with sufficient resources while ensuring that all fiscal requirements are fulfilled. (4 Activities)			
Regional Support	Regional Support	Provides leadership to the NCR as members of regional homeland security and emergency management leadership teams and supporting governance groups.	Daily Service
Mayor's Special Event Task Group (MSETG)	Mayor's Special Event Task Group (MSETG)	Manage the administration of the MSETG, a body responsible for organizing the City's public safety planning efforts for events requiring interagency coordination.	Daily Service
Grants Management	Serves as the State Administrative Agent for the federal homeland security grant programs that are awarded to the District of Columbia, and the National Capital Region (NCR)	Provides financial and programmatic oversight to various grant programs administered by DC HSEMA including emergency preparedness and response and recovery programs. Administers numerous individual subawards/projects in the District of Columbia and the National Capital Region.	Daily Service
COMMUNITY OUTREACH & MEDIA PREPARE	Community Outreach & Media Prepare	Maintain a strong outreach program designed to educate and equip community residents and businesses to prepare for and recover from all hazards and the potential for disasters.	Daily Service

Workload Measures

Measure	FY 2018 Actual	FY 2019 Actual	FY 2020 Actual
1 - Deployment for incident managment (3 Measures)			
Number of days agency staff are deployed out of District to support response and recovery activities in other jurisdictions	New in 2020	New in 2020	0
Number of days JAHOC teams are deployed to special events	New in 2020	New in 2020	12

Measure	FY 2018 Actual	FY 2019 Actual	FY 2020 Actual
Number of days agency staff are deployed to incident sites	New in 2020	New in 2020	167
1 - Emergency Operations Center (EOC) (4 Measures)			
Number of level 3 (enhanced) or higher Emergency Operations Center activations	5	4	13
Number of AlertDC messages sent to the public	New in 2020	New in 2020	9671
Number of HSEMA alerts sent to District government staff	New in 2020	New in 2020	4001
Alerts processed through JAHOC inbox	New in 2020	New in 2020	9729
2 - Tactical Analysis (2 Measures)			
Number of raw suspicious activity reports (SARs) processed	448	440	465
Number of requests for information (RFIs) processed	672	437	449
3 - Develop a suite of all hazard District preparedness plans in alignment with identified District Preparedness System capability priorities (1 Measure)			
Number of District plans created, revised, or reviewed for District Government partners annually	155	100	98
3 - Maintain the District's training and exercise plan in alignment with identified District Preparedness System capability priorities (1 Measure)			
Number of trainings provided to first responders, District employees, and the public by HSEMA	55	130	26
4 - Community Outreach & Media Prepare (1 Measure)			
Number of community preparedness trainings or events conducted by HSEMA	205	234	89
4 - Mayor's Special Event Task Group (MSETG) (1 Measure)			
Number of special events that have been processed by the Mayor's Special Events Task Group	116	92	48
4 - Serves as the State Administrative Agent for the federal homeland security grant programs that are awarded to the District of Columbia, and the National Capital Region (NCR) (3 Measures)			
Number of reimbursements processed for subrecipients annually	4025	3579	3227
Number of active subawards	New in 2020	New in 2020	1319
Number of grant monitoring visits	New in 2020	New in 2020	0

Strategic Initiatives

Strategic Initiative Title	Strategic Initiative Description	Proposed Completion Date
Capability Building (2 Strategic initiatives)		
Increase investment in resilient infrastructure and communities	In FY21, HSEMA will partner with additional agencies to successfully apply for increased mitigation funding from FEMA's new Building Resilient Infrastructure and Communities program.	09-30-2021
Expand the reach of HSEMA's community outreach program to high-risk communities	HSEMA will increase the preparedness of residents in neighborhoods at disproportionately higher risk of impact from natural and man-made hazards Specifically, HSEMA will conduct at least 10 community outreach events in wards 7 and 8 to advise residents of the specific risks to their communities and provide access to preparedness resources. Events may be conducted virtually or in person as needed to support COVID mitigation measures.	09-30-2021
Deployment for incident managment (1 Strategic Initiative)		
Inauguration	HSEMA will coordinate the District's agency-wide consequence management planning and execution for the 2021 Presidential Inauguration with District, regional, and federal partners, and develop the District's comprehensive after-action report. This will include coordination for both official Inauguration events as well as associated events including planned and unplanned demonstrations and other first amendment activity.	09-30-2021
Emergency Operations Center (EOC) (1 Strategic Initiative)		
EOC Renovation	In FY21, HSEMA will continue to upgrade the capabilities of the District's Emergency Operations Center (EOC). Working with the Department of General Services, HSEMA will complete the next phase of redesign of the EOC floor space to increase efficiency and maximize capacity during operations. HSEMA expects to complete the design phase and initiate the construction solicitation process by the end of FY21.	09-30-2021

Cyber Center

WEEKLY CYBER THREAT DIGEST

08 January 2020

Product No. 2020-01-001
NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

"Foot-in-the-Door" Techniques used to Elicit Personal Data

Online users are more likely to reveal private information based on how website forms are structured to elicit data. Researchers showed that by using digital "foot-in-the-door" techniques, such as requesting personal information from less private to more private (ascending privacy-intrusion order), websites can successfully entice users to reveal more of their private information. Similarly, by answering each request on consecutive, separate webpages, users reveal more private data. Websites can further manipulate their users by spreading out information requests over the course of several pages.

Data Leaks and Breaches

T-Mobile Customer Data Exposed

T-Mobile disclosed a breach last week revealing that it shut down "malicious, unauthorized access to some information" related to T-Mobile accounts. Specifically, that data consisted of customer proprietary network information (CPNI) that includes records of phone numbers that users called; the frequency, duration, and timing of such calls; and services that users purchased. T-Mobile said that the thieves in this case obtained phone numbers, subscribed lines, and call-related information. According to T-Mobile, the criminals did not access account names, physical or email addresses, financial data, credit-card information, Social Security numbers, tax ID, or passwords and PINs.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online identity theft resource page and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

PayPal Smishing Campaign Masquerades as Fraudulent Notification

A PayPal text message phishing campaign (smishing) is underway that attempts to steal users' account credentials and other sensitive information that can be used for identity theft. When PayPal detects suspicious or fraudulent activity on an account, it sets the account status to "limited," placing temporary restrictions on withdrawing, sending, or receiving money. This Paypal smishing campaign pretends to be from PayPal; it fraudulently states that the account has been permanently limited unless the user verifies their account by clicking on a link. The enclosed link brings the user to a phishing page that prompts them to log in to their account. The entered PayPal credentials are then sent to the threat actors. The phishing page then attempts to collect personal details on the user, including name, date of birth, address, bank details, and more.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim.

Malware Campaigns

Babuk Locker Debuts as First Enterprise Ransomware Of 2021

Babuk Locker is a new ransomware that launched at the beginning of 2021 and targets corporate victims in human-operated attacks. Cyber analysis has revealed that each Babuk Locker executable has been customized to each victim to contain a hardcoded extension, ransom note, and a darkweb accessible URL specific to the victim. A security researcher who also analyzed the new ransomware found that Babuk Locker's coding includes secure encryption that prevents victims from recovering their files for free. Once launched, the ransomware terminates various Windows services and processes known to keep files open and prevent encryption.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.

Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for financial gain or identity theft. Perpetrators take advantage of the numerous steps taken and parties involved in the real estate acquisition process. Read this NTIC Cyber Center report to learn about this prevalent scam and how to protect yourself.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-02-009

HSEC-1 | NTIC SIN No. 2.5, 5.4

February 6, 2020

National Capital Region Cyber Threat Spotlight

Iranian Threat Actors Using New Tools to Target Government Agencies and Private Organizations

Researchers at security firm Intezer believe that an Iranian threat group is using a new phishing campaign to compromise computers belonging to employees and customers of Westat, a company that provides contracting services to numerous US government agencies, state and local governments, and businesses. Researchers indicate that the threat actor, known as APT34, has sent Westat employees and customers emails that contain malicious documents disguised as surveys branded with Westat's logo. When opened, these documents deploy malicious tools, including a new backdoor malware known as TONEDEAF 2.0 and a new browser credential theft tool known as VALUEVAULT, which enable threat actors to issue remote commands via HTTP and steal information from compromised machines.

As Westat's customers include numerous agencies and organizations operating within the National Capital Region and elsewhere, this phishing campaign has the potential to pose a serious risk to many of our partners and members. ***Therefore, the NTIC Cyber Center advises employees of the above organizations to remain vigilant for phishing attempts associated with this or other cyber***

threat campaigns and to report any suspicious emails to your organization's IT security team. We also recommend IT administrators review Intezer's report and proactively block any associated Indicators of Compromise (IoCs).

Federal Partner Announcements

FBI Phone Number Spoofed in Social Security Scam

The FBI has seen a recent increase in phone calls that spoof the Bureau's phone number as part of a Social Security scam. The callers will often "spoof," or fake, the FBI Headquarters' phone number, 202-324-3000, so the call appears to be coming from the FBI on the recipient's caller ID. In this scam, fraudulent callers posing as an FBI agent inform victims that their Social Security numbers have been suspended. The scammer provides a fake name and badge number to trick victims into believing they are an FBI agent. The scammer tells victims that, to get their Social Security numbers reinstated, they must purchase gift cards, put money on the cards, and provide the scammer with the gift card numbers.

Please see the FBI's news release here for more information related to this threat. For additional information about these scams, please see the NTIC Cyber Center's blog posts on Social Security number suspension scams and neighbor number scams.

Current and Emerging Cyber Threats

Image of Kobe Bryant Deploys Cryptocurrency-Mining Malware

Security researchers at Microsoft Security Intelligence discovered cryptocurrency-mining – or crypto-mining – malware embedded in an HTML file that masquerades as downloadable wallpaper images of the late professional basketball player, Kobe Bryant. If the file is downloaded and opened, the crypto-mining malware will exploit the infected system's processor to illegally mine the cryptocurrency, Monero. Previous malicious cyber campaigns have embedded malware into celebrity photographs as well. ***The NTIC Cyber Center recommends always scanning files downloaded from the Internet with reputable antivirus software and refraining from downloading files from unknown or untrusted sources.***

Phishing Campaign Spoofs Spamhaus Correspondence

A researcher at Proofpoint discovered a new phishing campaign in which unknown threat actors delivered malware-laced emails masquerading as actionable notifications from the Spamhaus Project, an organization that generates spam block lists. The threat actors behind this campaign fraudulently warn victims that their email addresses have been added to a spam block list. Included in the email is a link labeled as instructions on removing emails from blacklists. However, this link leads to a malicious file that, if executed, will download and install the Ursnif Trojan, which can steal credentials and other data. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from the Spamhaus Project, avoid opening unexpected emails, and refrain from clicking on links and opening attachments from unknown or untrusted sources. If you receive this or a similar email in your work email account, notify your IT security team immediately.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Targeted Ransomware Attack on Electronic Warfare Associates

CyberScoop announced that Electronic Warfare Associates (EWA), a government contractor working with the US Department of Defense, the US Department of Justice, and the US Department of Homeland Security, was infected with Ryuk ransomware but has not yet issued any public statement about the incident. ZDNet discovered several EWA websites with what appeared to be encrypted files and ransom notes that can still be seen in cached Google searches even a week after EWA disconnected the infected web servers. Ryuk is often used to target high-profile organizations, Florida city's government network, resulting in large ransom payments. Ryuk ransomware is typically delivered through Emotet and Trickbot Trojan droppers to infect systems and spread through networks. ***As this appears to be an aggressive and rapidly evolving ransomware campaign, the NTIC Cyber Center would like to emphasize the importance of maintaining a robust and comprehensive data backup strategy to reduce downtime and recovery expenses that could result from a ransomware incident.***

DoppelPaymer Ransomware Operators Publishing Stolen Data

According to the associated dark web-based payment portal, DoppelPaymer ransomware operators are starting to publish data stolen from victims who do not remit payment. Discovered and analyzed in mid-2019 by CrowdStrike researchers, DoppelPaymer ransomware shares code with both the BitPaymer ransomware variant and the Dridex banking Trojan, providing it with the ability to both steal and encrypt data. While corresponding with the cybersecurity website BleepingComputer, the threat actors behind the DopplePaymer campaign claimed to have stolen data from victims for almost a year, selling some of the stolen files on the dark web when a victim refused to pay. While these threat actors claim that they have not yet publicly released any stolen data, it is likely they will adopt this tactic as similar campaigns show increased success in obtaining ransom payments from victims.

Vulnerabilities

Dell and HP Laptop Vulnerabilities

Cybersecurity firm Eclypsium published a report highlighting vulnerabilities present in Dell and HP laptops that, if exploited, could allow unauthorized privilege escalation through the devices' Direct Memory Access (DMA) capability. These vulnerabilities exist in Dell's XPS 13 7390 2-in-1 convertible laptop and HP ProBook 640 G4, including the HP Sure Start Gen4. HP has since released a BIOS update to mitigate this flaw and Dell has released the Dell Client BIOS to patch the issue. ***The NTIC Cyber Center recommends all users and administrators of vulnerable HP and Dell systems apply the appropriate updates as soon as possible. HP's update is available here and Dell's update is available here.***

Data Leaks and Breaches

A security researcher discovered a flaw in the social media management platform Social Captain that exposed the usernames and passwords of connected Instagram accounts. According to the researcher, unencrypted login credentials and other information from Instagram accounts connected to Social Captain could be viewed within the source code of the platform's profile pages. Since user ID values of Social Captain profile pages are assigned in sequential order, the researcher could modify the website's URL to view other Social Captain profile pages, including associated Instagram login credentials, without actually logging into the platform. ***The NTIC Cyber Center advises Social Captain users to disconnect their Instagram accounts from the management platform and immediately change any associated login credentials. We also encourage using lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Upcoming Webinars

Targeted Attacks: How Sophisticated Criminals Bypass Enterprise Security Measures

For close to three years, a technology executive was hounded by a persistent attacker who stole his identity, opened credit cards in his name, and wired funds from his bank account. Though SpyCloud

helped bring this particular criminal to justice, these tactics are common in targeted attacks.

If your account takeover prevention program primarily focuses on automated attacks like credential stuffing and password spraying, you may be leaving your organization exposed to serious losses. Targeted attacks are manual, creative, and elusive, making them one of the most difficult aspects of security and risk management. When criminals decide to go after high-value individuals and organizations, they're motivated to pull out all the stops, engaging in time-intensive, difficult to perpetrate methodologies in pursuit of lucrative rewards.

In this webinar, Chip Witt will dig into the tactics, techniques, and procedures (TTPs) criminals use to perpetrate highly-targeted attacks and identify areas where companies tend to invest unwisely in security technologies, leaving them vulnerable to sophisticated attackers. He will:

- Walk through the timeline of a breach and what types of attacks are prevalent at each stage
- Examine the advanced tactics criminals use to bypass enterprise security measures
- Give you perspective on why enterprises should be more concerned about targeted versus automated account takeover attacks
- Share steps you can take to bolster your defenses and protect against the most damaging attacks

To register for this free webinar on Tuesday, February 11 at 11:30 AM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Rental scams are a type of social engineering scheme in which perpetrators advertise fake apartment, condominium, home, or vacation rental listings with the intent of defrauding those seeking to lease such properties. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Leaked Documents Expose the Secretive Market for Your Web Browsing Data
Analytic Comment: Motherboard and PCMag conducted a joint investigation revealing that

antivirus vendor, Avast, collected user browsing data and sold it through its own subsidiary, Jumpshot. Avast collected data such as user location, Google Searches, and visited URLs, including browsing data linked to adult websites. While Avast stated that users had to opt-in for data collection and that the information was anonymized and could not identify specific individuals, other sources claim otherwise. A few months ago, another security researcher claimed that Avast's browser plugin harvested web browsing data. Avast has since discontinued Jumpshot's operations. This incident demonstrates the importance of fully reading and understanding a company's terms of service (ToS) or end user license agreement (EULA) prior to installing any software or application and maintaining awareness of data collection practices employed by many companies and organizations.

Ransomware Linked to Iran, Targets Industrial Controls

Analytic Comment: Cybersecurity firm Otorio recently discovered a new strain of ransomware, dubbed SNAKE, that targets industrial control systems (ICS). The malware, believed to be of Iranian origin, searches for and encrypts files associated with programs that control industrial processes, crippling manufacturing companies and preventing analysis, configuration, and control of ICS. SNAKE was recently used in conjunction with data wiping malware in a January 2020 attack on Bahrain Petroleum Company, an oil and gas company believed to be targeted by Iran as retaliation for regional strife over oil prices. This incident should serve as a reminder that Iranian actors have employed powerful cyber capabilities against political adversaries and are likely continue to do so against US targets in light of the recent escalation in US-Iranian political tensions.

Patches and Updates

Adobe Releases Security Updates for Magento

Cisco Releases Security Updates for Cisco Small Business Switches

Google Releases Security Updates for Chrome

OpenSMTPD Vulnerability

ICS-CERT Advisories

AutomationDirect C-More Touch Panels

Medtronic Conexus Radio Frequency Telemetry Protocol (Update A)

Medtronic 2090 Carelink Programmer Vulnerabilities (Update C)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-02-020

HSEC-1 | NTIC SIN No. 2.5, 5.4

February 13, 2020

National Capital Region Cyber Threat Spotlight

Scam Calls Threatening Pending Court Cases Target Local Residents

According to a Tweet posted by Leesburg Police on February 7, 2020, residents in the Virginia counties of Leesburg and Loudoun recently reported receiving scam telephone calls from someone claiming to be a process server with Loudoun Circuit Court. The calls, which appear to be automated, try to trick recipients into believing that there is a pending case against them in Loudoun Circuit Court. The caller claims that a process server had already tried to establish contact with the recipient at his or her home and threatens that recipients who do not respond to the calls will lose their rights in the supposed court case. The Leesburg Police Department, Loudoun County Sherriff's Office, and Loudoun Circuit Court Clerk's Office warn that these claims are fraudulent and advise

residents who receive them to report the scam to their local law enforcement entity. ***As this or other scam campaigns could evolve in tactics or expand to target additional residents within the National Capital Region, the NTIC Cyber Center advises members to remain vigilant for phone calls or other forms of communication spoofing threatening action from law enforcement or government agencies. In addition, we advise readers to consult our Security Our Communities blog series to learn about similar scams and the strategies for protecting against them.***

Current and Emerging Cyber Threats

Iranian-Linked Phishing Attackers Pose as Journalists

A UK-based research group has reported numerous spear phishing campaigns in which Iranian-linked attackers pose as journalists from various news publications such as the Wall Street Journal, CNN, and Deutsche Welle, among others. These phishing emails promise recipients an interview with a veteran journalist and then instructs them to input their Google password to view the interview questions. Cybersecurity researchers believe this attack originated from a group dubbed Charming Kitten, an Iran-linked advanced persistent threat (APT) group that previously targeted a US presidential campaign. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as media representatives and journalists, avoid opening unexpected emails, and refrain from clicking on links and opening attachments from unknown or untrusted sources. If you receive any suspicious email in your work email account, notify your IT security team immediately.***

Tax-Themed Phishing Emails Used to Distribute Emotet

Security researchers at Cofense warn that attackers are distributing the Emotet Trojan through spam emails disguised as tax correspondence. The emails spoof W-9 tax forms and contain malicious macro-enabled Microsoft Word attachments that, when opened, infect systems with Emotet, a dangerous banking Trojan that can steal network and account login credentials and download additional malware onto an infected system, such as ransomware. The NTIC Cyber Center advises users to remain vigilant for tax-themed malware campaigns. Furthermore, since exploiting Microsoft Office macro functionality to deliver malicious payloads is a common attack vector, ***the NTIC Cyber Center recommends that users disable Microsoft Office macros by default, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. Lastly, we encourage readers to reference our blog post on IRS tax scams for additional information on tax-related campaigns that may target individuals during this year's tax season.***

Campaign Exploiting Bitbucket's Online Code Repositories to Drop Malware

Cybereason research analysts have been tracking an active and ongoing malware campaign that exploits BitBucket, an online code repository, to spread several types of malware to a large number of unsuspecting victims. This campaign distributes seven different types of malware including ransomware, crypto-mining malware, and data-stealing malware that targets login credentials, web browser cookies, two-factor authentication tokens, and cryptocurrency wallets. Researchers estimate that approximately 500,000 devices have been infected by so far. This campaign's objective appears to be financially-motivated as the payloads used in this campaign are designed to maximize revenue for the attackers. This campaign primarily impacts people who download free commercial software products. Researchers have yet to determine a specific threat actor or group behind this campaign. ***The NTIC Cyber Center recommends refraining from downloading "free" or "cracked" versions of expensive software as they can and often do contain malware. We recommend only downloading software and applications from reputable vendors. Lastly, be sure to use a reputable antivirus solution and keep it and all software and operating systems patched and updated.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Vulnerable Gigabyte Drivers Used to Spread RobbinHood Ransomware

Security researchers at Sophos have observed RobbinHood ransomware actors using vulnerable drivers from hardware and software company Gigabyte to circumvent antivirus protections and install ransomware onto targeted machines. According to the research, the ransomware actors install Gigabyte drivers known to be vulnerable to CVE-2018-19320 and exploit the vulnerability to push the installation of malicious kernel drivers. In turn, the actors use the kernel drivers to kill processes associated with endpoint security protections and spread ransomware without interference from antivirus solutions. ***The NTIC Cyber Center advises administrators review the Sophos report for mitigation strategies and IoCs associated with this emerging campaign.***

New Mailto/Netwalker Ransomware Impersonates "Sticky Password" Software

Researchers at ID Ransomware have spotted a sophisticated new ransomware variant, dubbed both Mailto and Netwalker, named after the extension appended to encrypted files and the associated decryption tool, respectively. Mailto/Netwalker targets Windows devices on enterprise networks, but its distribution method is currently unknown; however, researchers discovered that the payload is an executable file that impersonates “Sticky Password” software and will execute after any user interaction. This ransomware makes no attempt to remain subtle, and quickly encrypts the user’s data as soon as the ransomware executes. Once executed, Mailto/Netwalker encrypts targeted files and drops a ransom note containing two email addresses that victims can use to contact the attacker and obtain instructions for payment and the ransom amount. There is currently no publicly available decryption tool for this variant. Bleeping Computer provides more information about Mailto/Netwalker here.

SaveTheQueen Ransomware Propagates through Compromised SYSVOL Folder

Researchers discovered a new strain of ransomware that appends encrypted file names with the extension .SaveTheQueen and uses the SYSVOL share on a domain controller to spread within a network. SYSVOL is a domain controller folder that handles numerous synchronization processes with connected domain clients. After obtaining administrative privileges on the domain controller, attackers managed to write to the SYSVOL folder and run PowerShell scripts on endpoints to spread the ransomware. For more information on this new ransomware campaign, see Varonis’s report here.

Vulnerabilities

A Vulnerability in Philips Hue Smart Light Bulbs

Security researchers at Check Point discovered a vulnerability in Philips Hue smart lightbulbs and its bridge module that can be exploited by remote threat actors to compromise the victim's home network and execute arbitrary code. The vulnerability, tracked as CVE-2020-6007, has a severity score of 7.9 out of 10 as it can allow attackers to hack into and exploit other devices that reside on the same network. Philips Hue's parent company Signify released a patch for the vulnerability in firmware version 1935144040. ***The NTIC Cyber Center recommends Philips Hue smart lightbulb users to update the firmware to the latest version. We also recommend monitor home networks for***

unusual and suspicious activity.

Vulnerability in Dell's SupportAssist Diagnostic Software

A researcher at Cyberark reported a vulnerability that allows the execution of arbitrary code in SupportAssist, a diagnostic software that is preinstalled on most newer Dell systems with Windows OS. The vulnerability, tracked as CVE-2020-5316, has a severity score of 7.8 out of 10 as it can allow local attackers to abuse dynamic link libraries (DLLs) for the execution of arbitrary code with administrator privileges. Dell released a patch for the vulnerability for home PCs running SupportAssist version 3.4 or earlier and business PCs running version 2.1.3 or earlier. Users who do not have SupportAssist auto-update enabled can do so via the settings window in the "About SupportAssist" section. Business customers are encouraged to view the instructions here for additional guidance. ***The NTIC Cyber Center recommends affected Dell users to update SupportAssist to the latest version.***

Industry Report

Palo Alto Unit 42 Cloud Threat Report

Cloud computing is now at the center of nearly every business strategy. But, as with the rapid adoption of any new technology, growing pains persist. To help organizations achieve secure cloud computing and innovation, the cloud-focused division of Unit 42 has released the Spring 2020 edition of their bi-annual Unit 42 Cloud Threat Report. Based upon threat intelligence from multiple data sources, including publicly available data and proprietary data from Palo Alto Networks, the key findings shed light on security missteps that are actually in practice by organizations across the globe.

This report is available for free via Palo Alto Networks' website here.

Data Leaks and Breaches

Fifth Third Bank has announced a breach of data impacting a limited number of customers. According to the bank's disclosure statement, several former employees stole personal information belonging to an undisclosed number of customers and provided it to a third party. Information exposed in this breach includes customer names, Social Security numbers, driver's license information, mother's maiden names, addresses, phone numbers, dates of birth, and account numbers. Though the bank has issued notifications to affected individuals, ***the NTIC Cyber Center encourages all Fifth Third customers to monitor their account statements and immediately notify their financial institutions of any suspicious or unauthorized activity. In addition, we advise customers to remain vigilant for a possible increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Who's In Your Cloud?
How Privileged Access Controls are Leaving You Exposed

Managing who has access to your cloud environment is mission-critical for IT security. Compliance is putting pressure on how organizations manage privileged access on these systems, which are storing petabytes of user and customer data.

Unfortunately, the nature of Linux makes it very hard to understand who is in your cloud at any given moment - resulting in breach detection times of over 200 days. Legacy solutions for privileged access management (PAM), designed to address this problem on Windows, completely neglect the Linux platform and leave you exposed.

Join Cmd's Head of Security, John Brunn, to learn the nature of these failures, why it's so difficult to understand and locate who is in your cloud, and how to fix it. You will learn:

- How to assess your gaps in user attribution and compliance on Linux
- Why requirements for PAM on Linux are different than Windows
- What a PAM solution for Linux should be designed to do

- How to execute a smart PAM strategy in your Linux cloud

To register for this free webinar on Wednesday, February 19 at 2:00 PM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Romance scam is a social engineering scheme where a perpetrator masquerades as a potential love interest, concealing his or her true intentions to elicit money or material possessions from unsuspecting victims looking for love online. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

When Your Used Car Is a Little Too 'Mobile'
Analytic Comment: The previous owner of a leased Ford vehicle recently discovered he was still able to use Ford's online customer dashboard to access certain features of his former car despite having surrendered ownership of it when his lease expired four years ago. Using the myFord mobile platform, the owner found that his credentials still allowed him to track the location of the vehicle, read its mileage statistics, remotely start the vehicle, and lock and unlock its doors. A spokesperson for Ford believed the oversight occurred after a dealership failed to perform a "master reset" to remove associated account owner information from the vehicle's Internet-connected systems. This security incident highlights the need for both organizations and consumers to exercise responsible stewardship of personal information stored on Internet of Things (IoT) devices and underscores the importance of taking proactive measures to disassociate personal information from devices or services when accounts are terminated or ownership is transferred.

Iowa Caucus App Has Security Flaws, Hackers Could Change Passwords, Vote Tallies: Report
Analytic Comment: Cybersecurity firm Otorio recently discovered a new strain of ransomware, dubbed SNAKE, that targets industrial control systems (ICS). The malware, believed to be of Iranian origin, searches for and encrypts files associated with programs that control industrial processes, crippling manufacturing companies and preventing analysis, configuration, and control of ICS. SNAKE was recently used in conjunction with data wiping malware in a January 2020 attack on Bahrain Petroleum Company, an oil and gas company believed to be targeted by Iran as retaliation for regional strife over oil prices. This incident should serve as a reminder that Iranian

actors have employed powerful cyber capabilities against political adversaries and are likely continue to do so against US targets in light of the recent escalation in US-Iranian political tensions.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Cisco Releases Security Updates for Multiple Products

Intel Releases Security Updates

Microsoft Releases February 2020 Security Updates

Mozilla Releases Security Updates for Multiple Products

ICS-CERT Advisories

Siemens Industrial Products SNMP Vulnerabilities

Siemens OZW Web Server

Siemens PROFINET-IO Stack

Siemens SCALANCE S-600

Siemens SCALANCE X Switches

Siemens SIMATIC CP 1543-1

Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC

Siemens SIMATIC S7

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

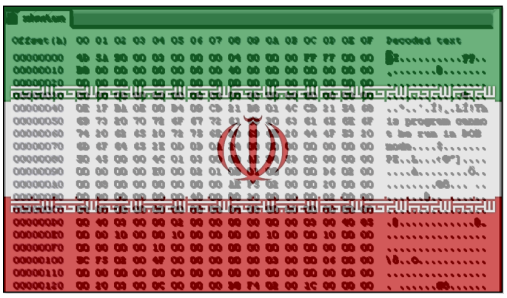
Product No. 2020-02-029

HSEC-1 | NTIC SIN No. 2.5, 5.4

February 20, 2020

National Capital Region Cyber Threat Spotlight

Iranian Cyber Groups Targeting Vulnerable VPN Systems to Enable Surveillance and Other Attacks



New research from cybersecurity firm ClearSky suggests that Iranian-backed cyber threat groups move quickly and aggressively to attack vulnerable virtual private network (VPN) servers, often within mere hours after vulnerabilities are publicly disclosed. In 2019, these actors targeted vulnerable VPN servers from providers including Pulse Secure, Palo Alto Networks, Fortinet, and Citrix to breach organizations within the IT, telecommunications, oil and gas, aviation, government, and security sectors. After gaining initial entry, the attackers were observed using both existing system administrator utilities and custom tools to move laterally through networks and enable backdoor access for surveillance operations. Researchers believe these tactics could be also be weaponized to perpetrate supply-chain attacks or deploy data-wiping malware to destroy information on targeted networks.

As this report highlights the advanced technical capabilities of Iranian nation-state cyber actors to quickly infiltrate organizations through vulnerable VPN platforms, the NTIC Cyber Center reminds administrators to move expeditiously when updating systems with the latest security

patches in order to ensure protection against network intrusions, ransomware, and other cyber threats as soon as possible. Additionally, we advise administrators to review ClearSky's report and proactively block any indicators of compromise (IoCs) associated with these campaigns. For additional information on Iranian cyber threat campaigns, please reference the NTIC Cyber Center's product on Iran's cyber capabilities here.

Federal Partner Announcement

IRS Advises Enabling Multifactor Authentication on Tax Preparation Products

The Internal Revenue Service (IRS) has issued a news release advising tax professionals and taxpayers to implement multi-factor authentication (MFA) on tax preparation software products. MFA provides an extra layer of security to online accounts by allowing customers to secure their accounts against fraudulent login attempts using unique codes delivered through email, text message, or phone call. The IRS advises that enabling MFA on tax preparation products could help combat against identity theft and data theft, which, according to the IRS, has already affected nearly two dozen tax practitioner firms this tax season. The IRS believes it is particularly important to secure tax preparation products with MFA because of the sensitive nature of the information stored in both the software and in associated online accounts. The IRS also warns of the dangers of tax-themed phishing scams that attempt to trick recipients into downloading attachments or opening malicious links and ultimately enable the theft of sensitive information, the distribution of ransomware, or other malicious attacks.

The NTIC Cyber Center advises users of tax preparation software to enable MFA on all accounts that offer it and to consult the IRS's resources for more information on reducing the risk of identity theft. In addition, we remind users to remain vigilant for phishing emails disguised as tax-related correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources.

Current and Emerging Cyber Threats

SMS Messages Lead to Fake Mobile Banking Websites

Security researchers from Lookout recently discovered an automated SMS phishing campaign that targeted mobile banking users and utilized over 200 webpages designed to spoof mobile versions of legitimate banking websites. This campaign took advantage of users who regularly received SMS messages from their banks, using similar and familiar messaging to entice victims to click on links and enter sensitive information such as the answers to specific security questions, account numbers, and card expiration dates. Banks exploited in this campaign included Chase, TD, BNC, RBC, Scotiabank, CIBC, UNI, HSBC, Tangerine, Meridian, Laurentian, and Manulife. Although this particular campaign is no longer active and Lookout has contacted all affected banks, similar campaigns will likely surface in the future. For this reason, ***the NTIC Cyber Center reminds our readers to visit banking and other websites containing sensitive personal information through the company's official mobile application or by typing the web address directly into a web browser. To reduce the risk of becoming a victim of a this or any other type of phishing attack, refrain from clicking on links or opening attachments from unexpected messages or unknown sources.***

Spear Phishing Attack Using SLK Attachments

Researchers uncovered a spear phishing email campaign targeting the employees of thirteen major international companies with malicious attachments. Threat actors behind this campaign masquerade as the targeted company's clients or vendors and send business transaction email correspondence with an attached Excel Symbolic Link (SLK) file containing malicious macros. If these attachments are opened and macros are enabled, the NetSupport Manager remote access trojan (RAT) will infect the recipient's system and create a backdoor, allowing threat actors to have remote access to the targeted computer and other assets on the same network. ***The NTIC Cyber Center recommends never opening or enabling macros in attachments on unexpected or unsolicited documents, disabling macros by default on Microsoft Office applications, and keeping all software, operating systems, and antivirus solutions updated.***

Malicious VPN Advertising Campaign

Researchers discovered a malicious advertising – or malvertising – campaign attempting to infect visitors with AZORult information-stealing malware. This campaign attempts to lure victims to protonvpn[.]store, a fraudulent website masquerading as the virtual private network service provider ProtonVPN to get victims to download a malicious payload disguised as the VPN's installer. If downloaded, the payload installs the AZORult Trojan designed to exfiltrate sensitive user data to its operators and may act as a downloader for other malware families. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and running reputable and up-to-date antivirus software. We also recommend network administrators***

reference and block the associated indicators of compromise (IoCs) contained in Precisionsec's report.

Vulnerabilities

SweynTooth Vulnerabilities Impact Many Bluetooth-Enabled Devices

Three security researchers from the Singapore University of Technology and Design have discovered a several flaws, collectively dubbed SweynTooth, in Bluetooth Low Energy technology present on several system-on-a-chip (SoC) circuits within at least 480 products from different vendors. If exploited, these vulnerabilities can allow attackers within the device's Bluetooth range to bypass the secure Bluetooth pairing mode and gain access as an authorized user on that device. This is of particular concern to the healthcare sector as some Bluetooth-enabled pacemakers, inhalers, and blood glucose meters are also impacted by these vulnerabilities. Although these vulnerabilities are not currently considered to be critical or severe, ***the NTIC Cyber Center recommends administrators of affected Bluetooth-enabled devices apply patches if and when they become available. For more information about these vulnerabilities and to see a list of affected devices, please see BleepingComputer's article here***

ThemeGrill Demo Importer Plugin Vulnerability

Security researchers warn that a vulnerability identified in the WordPress plugin "ThemeGrill Demo Importer" could allow attackers to wipe data stored in databases and assume administrator control of vulnerable websites. This vulnerability affects versions 1.3.4 to 1.6.1 of the plugin and is believed to be particularly dangerous as its successful exploitation does not require a malicious payload and cannot be blocked by firewall protections. Researchers believe up to 200,000 WordPress sites may currently be at risk of attack as a result of this vulnerability. ***The NTIC Cyber Center encourages administrators of WordPress websites that have the ThemeGrill Demo Importer plugin installed to immediately upgrade to the latest version, 1.6.3, and maintain regular website backups that are stored securely off the network.***

Data Leaks and Breaches

Rutter's, a convenience store chain with locations in Pennsylvania, Maryland, and West Virginia, reported a data breach in which unknown threat actors placed information-stealing malware on the company's payment processing systems, potentially affecting all customers who used payment cards at in-store and fuel dispenser point-of-sale (PoS) terminals between September 20, 2018 and May 29, 2019. Rutter's believes that this malware allowed cyber criminals to steal customer data including cardholder names, payment card numbers, expiration dates and internal verification codes during the affected time period. However, transactions processed through the in-store chip-enabled (EMV) PoS terminals only compromised card numbers and expiration dates and did not include cardholder names or verification codes. Rutter's states that transactions involving car washes, lottery machines, and in-store ATMs were not affected. Rutter's has since remediated its PoS systems. ***The NTIC Cyber Center recommends customers who used payment cards at any Rutter's location within the affected timeframe monitor their account statements and immediately notify their financial institutions of any unauthorized activity.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification. TODAY

Connected Intelligence: The Future of Fraud Defense

In today's digital world, fighting fraud requires a dynamic approach that connects multiple layers of security and leverages a coordinated set of AI-based solutions to continuously stay on top of the newest fraud schemes while preserving a seamless consumer experience.

Register for and attend this live webinar and you will learn:

- How a Connected Intelligence approach to security can link different points of consumer interaction - from login to checkout and beyond;
- The benefits that this approach can have on your user experience;
- How to get started in implementing a more connected security strategy.

To register for this free webinar on Wednesday, February 26 at 2:00 PM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Tuition scams are clever social engineering schemes designed to trick unsuspecting prospective, current, or former college students into willingly and unnecessarily paying money to obtain some type of financial assistance for their education costs. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Blockchain Voting App Is Dangerously Vulnerable, Researchers Say

Analytic Comment: Researchers from the Massachusetts Institute of Technology (MIT) have identified several vulnerabilities in the blockchain voting application Voatz that could allow attackers to observe, suppress, or alter votes cast on compromised devices. In addition, the researchers believe that attackers could also compromise Voatz's servers and alter ballots centrally through the app's application programming interface, or API. Voatz, however, has disputed these claims, contending that the vulnerabilities were found in an outdated version of the app and that protections exist to prevent the type of unauthorized server access described in the researchers' attack scenario. Cybersecurity concerns surrounding Voatz and other Internet-based voting platforms, such as the app used during Iowa's recent caucus event, underscore the importance of performing proper vulnerability tests and security assessments on these products in advance of their release and use, especially as the 2020 elections approach.

State Agencies Urged to Move Beyond Login Credentials to Counter Cyber Risks

Analytic Comment: IT leaders within state and local agencies are being directed to make identity and access management controls more of a priority due to recent attacks and breaches. According to one survey, 87 percent of state chief information security officers said that implementing a multi-factor authentication (MFA) solution would be their top choice for the new directive. Username and password combinations are often considered the lowest hanging fruit for threat actors conducting phishing campaigns. Since state and local governments primarily use only username and password combinations for account access, adding MFA would add another layer of protection. This underscores the need to shift from reliance on conventional username and password combinations for securing account access toward implementing MFA to enable stronger authentication on all online services and websites.

Patches and Updates

VMware Releases Security Updates for vRealize Operations for Horizon Adapter

ICS-CERT Advisories

Emerson OpenEnterprise

GE Ultrasound products

Honeywell INNCOM INNControl 3

Interpeak IPnet TCP/IP Stack (Update C)

Schneider Electric Magelis HMI Panels

Schneider Electric Modicon Ethernet Serial RTU

Spacelabs Xhibit Telemetry Receiver (XTR)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-02-042

HSEC-1 | NTIC SIN No. 2.5, 5.4

February 27, 2020

National Capital Region Cyber Threat Spotlight

Malicious Spam Looking to Steal Tax Data

Researchers at Proofpoint observed multiple methods in which threat actors are attempting to steal data this tax season. Along with conventional tactics that include malicious spam (malspam) campaigns that contain malware-laden attachments and spear phishing emails that masquerade as official correspondence to steal login credentials, threat actors tactics have evolved to leverage legitimate applications such as TeamViewer to bypass security filters. TeamViewer is a remote access software solution that is often abused by cyber threat actors to access and control a victim's computer. Since TeamViewer is a legitimate application and can be embedded within compromised websites and attached documents, it often goes undetected by antivirus software. Smaller tax-preparation organizations are increasingly targeted and exploited in these campaigns as they are less likely to have defenses in place to thwart these attacks. ***The NTIC Cyber Center recommends users remain vigilant for malspam or spear phishing campaigns disguised as official tax correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you***

receive an email or visit a tax preparation website that you suspect may be malicious, contact the company via another communication method, such as a phone call, to verify legitimacy.

Current and Emerging Cyber Threats

MageCart Discovered on More Websites

Security researchers uncovered a recent malicious campaign designed to steal bank card information from unsuspecting customers making online payments. Cyber threat actors, dubbed "MageCart Group 12," have infected nine websites with malicious JavaScript running a card skimmer that steals payment card information. Researchers attempted to contact the owners of the infected websites but received no response. A list of impacted websites is available via BleepingComputer. ***The NTIC Cyber Center recommends that customers who may have made purchases via the impacted websites during the affected time frames monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. We also recommend all website administrators monitor their sites for unauthorized changes, secure administrator accounts with multifactor authentication, and keep associated ecommerce platforms updated with the latest versions.***

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Premium WordPress Theme/Plug-ins Infected with Malware

Researchers at Prevailion, a security intelligence company, are analyzing an ongoing malware threat that is responsible for infecting over 20,000 premium WordPress theme and plugin users. Once the user downloads the theme or plugin, it installs a Trojan containing command and control communication functions allowing the threat actor to remotely execute malicious code and add an administrative account. This account allows the attacker to manipulate anti-adblocker scripts, capture cookies from all visitors, add malicious advertisements on the compromised website, and redirect visitors to pages containing exploit kits. This campaign attempts to maintain persistence on affected websites by adding its malicious code to multiple files on the web server, ensuring the threat remains even after an administrator deletes the offending code from the initial loading stage. ***The NTIC Cyber Center encourages administrators of WordPress websites that have themes and plugins installed to immediately upgrade to the latest version and maintain regular website backups that are stored securely off the network.***

Haken Malware Signs Android Users up for Expensive Subscriptions

Eight Android apps recently available for download from the official Google Play store have been identified as containing a new malware variant named Haken that retrieves sensitive data from victims and covertly signs them up for an expensive premium subscription. These apps functioned as camera utilities and children's games but ran a multitude of malicious functions in the background and could access any sensitive information visible on the mobile screen from emails, text messages, pics and any apps or browsers the victim uses. Haken has a clickable capability that imitates user interaction by clicking anything that appears anywhere on the screen of the device. This allows Haken to bypass permissions and add code into advertising monetization platforms for Facebook Ad Center and for Google AdMob, giving the attackers access to payment cards associated with these accounts. ***Although these eight malicious apps were removed from the Play store after researchers notified Google, the NTIC Cyber Center recommends all Android users remain vigilant for this type of device behavior after installing any new mobile app and monitor financial account statements for suspicious and unauthorized activity. We also recommend thoroughly reading user reviews and ratings prior to downloading and installing any new app to help determine its legitimacy.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

DoppelPaymer Now Threatens to Publish Victims' Data

DoppelPaymer ransomware operators have opened a public-facing website to publish data stolen from victims who do not remit payment. Discovered and analyzed in mid-2019 by CrowdStrike researchers, DoppelPaymer ransomware shares code with both the BitPaymer ransomware variant and the Dridex banking Trojan, providing it with the ability to both steal and encrypt data. While corresponding with members of the cybersecurity website BleepingComputer, the threat actors behind the DopplePaymer campaign claimed that the public site is in "test mode," used publish a few stolen files for shaming. Currently, data from four victims are posted on this site and these threat actors claim they plan on performing more data exfiltration activities.

Vulnerabilities

Honeywell Fire Alarm Systems

Researchers at Applied Risk discovered two vulnerabilities in Honeywell's fire alarm systems that, if exploited, could allow unauthorized access to the alarm system's functions. The first vulnerability, tracked as CVE-2020-6972, can allow attackers to bypass authentication on the alarm system's web server, providing access to the administrator dashboard and the alarm system's functionality. The second vulnerability, tracked as CVE-2020-6974, exposes a database containing sensitive information such as usernames and password hashes associated with the fire alarm systems. CISA has rated these vulnerabilities as critical in ICS Advisory ICSA-20-051-03. ***The NTIC Cyber Center recommends all affected users log into their Honeywell account for more information and update their systems' firmware as soon as possible.***

Zyxel Network Storage Devices

KrebsOnSecurity recently notified networking hardware vendor Zyxel about a critical vulnerability in the company's network attacked storage (NAS) devices. This vulnerability, if exploited, allows attackers to access devices remotely without any interaction from authorized users. CERT rates this vulnerability as severe. Twelve days after being notified, Zyxel released firmware updates for affected devices. ***The NTIC Cyber Center recommends users and administrators of Zyxel devices review the CERT Vulnerability Note and apply the appropriate firmware updates as soon as possible.***

Data Leaks and Breaches

The Defense Information Systems Agency (DISA) recently disclosed a beach affecting 200,000 individuals in which personally identifiable information (PII), including Social Security numbers may have been exposed. The breach occurred between May 2019 to July 2019. DISA did not specify how the database was compromised but did state that there was no evidence to suggest that any of the potentially compromised PII was misused. ***The NTIC Cyber Center encourages those***

affected to consider placing a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring services offered to affected personnel and enabling multi-factor authentication (MFA) on all accounts that offer it.

MGM confirmed a data breach that resulted in the exposure of personal information for 10.6 million MGM hotel guests that was recently published on a hacking forum. MGM representatives stated that data came from a security incident last year and that no financial, payment card, or password data was affected. Information exposed in the breach includes hotel guest names, home addresses, email addresses, phone numbers, and dates of birth. ***The NTIC Cyber Center recommends that MGM hotel guests who stayed with MGM during the affected time period remain vigilant for phishing emails and refrain from clicking on links from unknown or untrusted sources.***

Mobile device case retailer, Slickwraps, recently disclosed a data breach that resulted in the exposure of personal customer information regarding purchases made on Slickwrap's webstore before February 21, 2020. The breach is attributed to an unknown threat actor who leveraged an exploit to access non-production databases, making them publicly accessible. Compromised information includes customers' names, emails, and addresses. Slickwraps states that no personal financial data or passwords were compromised and customers who checked out as "GUEST" were not victimized in this breach. Slickwraps has since closed the exposed databases. ***The NTIC Cyber Center recommends that Slickwrap customers change their accounts' login credentials and remain vigilant for phishing emails.***

Security company, UpGuard, discovered a publicly exposed cloud database containing personal data and behavioral profiles of 120 million Americans. The 747 GB database belonged to Tetrad, a market and behavior analysis firm, which contained customer information from clients such as Experian, Kate Spade, and Bevmo. The data was exposed for an undetermined amount of time and included American names, genders, addresses, and customer "types." Tetrad has since secured the

database and stated that the exposed information could not be used for financial or identity fraud. ***The NTIC Cyber Center recommends readers to remain vigilant for phishing emails and refrain from clicking on links from unknown or untrusted sources. We also recommend reviewing and comprehending the terms of service before using any service.***

Upcoming Webinars

Data Breach TODAY®
Prevention. Response. Notification.

Risk Exchanges: The Key to Vendor Risk Management Efficiency in NA

Your vendors often handle your most sensitive data. This presents new challenges as third-party risk, security, privacy, legal and IT teams struggle to vet and manage the vendors they rely on most. We'll discuss emerging vendor management trends and breakdown how risk exchanges are key to more efficient business operations.

Join this webinar where you'll learn:

- The emerging vendor risk management trends and challenges
- How risk exchanges can help streamline vendor due diligence
- Why risk exchanges are the secret to vendor risk and performance monitoring

To register for this free webinar on Wednesday, February 2 at 2:00 PM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Business Email Compromise (BEC) – also known as a CEO scam or whaling – is a type of phishing scheme in which the perpetrator conducts online reconnaissance against a target organization and then uses various social engineering techniques to try and convince employees within that organization to divulge sensitive personal or financial information Click here to read more about this prevalent scam and learn how to protect yourself

---

Cyber in the News

Wanted: Hands-On Cybersecurity Experience

Analytic Comment: As cyber threats become increasingly prevalent, the funding and focus on layers in defense-in-depth put a gap in-between a need to hire in the cybersecurity field versus qualified candidates with hands-on experience. Data gathered from over 2,00 responders in more than 100 countries reveal that over half of responders believe their cyber teams are understaffed and 73 percent are not satisfied with new applicants. One-third of employers state that non-security skills such as communication, social, and leadership skills increase this gap as it is necessary to be able to articulate a possible impact of a vulnerability or threat precisely and professionally. With almost 80 percent of organizations needing to expand and restructure their cyber infrastructure within the next 12 months, current and expected cyber professionals should maintain a current working knowledge on as many tools and threats as possible while improving their communication skills.

Governors Push Congress for Increased Cybersecurity Funding

Analytic Comment: In response to the upsurge of cyber attacks across the nation, the National Governors Association (NGA) is urging Congress to pass legislation for more grant funding for states and local municipalities. A recent report by security firm Emsisoft estimated that ransomware affected at least 966 government entities, educational institutions, and healthcare providers last year. Furthermore, according to the Research and Technology Subcommittee, the lack of skills and education contribute to vacant cybersecurity positions. This underscores the importance of proper cybersecurity related funding so that vulnerable organizations may pay for properly trained personnel.

Patches and Updates

Adobe Releases Security Updates for After Effects and Media Encoder

Cisco Releases Security Updates

Google Releases Security Updates for Chrome

Google Releases Security Updates for Chrome

OpenSMTPD Releases Version 6.6.4p1 to Address a Critical Vulnerability

---

ICS-CERT Advisories

Auto-Maskin RP210E, DCU210E, and Marine Observer Pro (Android App)

B&R Industrial Automation Automation Studio and Automation Runtime

Honeywell NOTI-FIRE-NET Web Server (NWS-3)

Honeywell WIN-PAK

Moxa EDS-G516E and EDS-510E Series Ethernet Switches

Moxa ioLogik 2542-HSPA Series Controllers and IOs, and IOxpress Configuration Utility

Moxa MB3xxx Series Protocol Gateways

Moxa PT-7528 and PT-7828 Series Ethernet Switches

Rockwell Automation FactoryTalk Diagnostics

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-03-008

HSEC-1 | NTIC SIN No. 2.5, 5.4

March 5, 2020

National Capital Region Cyber Threat Spotlight

Ransomware Campaigns Increasingly Steal Victims' Data Prior to Encryption

Although we regularly report new and evolving ransomware campaigns in our bulletins, this week, we decided to highlight a growing tactic that ransomware operators are increasingly using to coerce victims into paying the ransom. Previous ransomware campaigns relied upon merely encrypting victims' data in the hopes that the potential for permanent data loss would be enough of an incentive to pay the ransom. However, as awareness of this threat increased and organizations began implementing more robust data backup procedures, sophisticated ransomware campaigns evolved and many have begun stealing victims' data prior to encrypting it, threatening to release the stolen data publicly if the ransom demand is not met. Ransomware campaigns such as Sodinokibi/REvil, Maze, Nemty, BitPyLock, and DoppelPaymer have all recently added a data theft component to their attacks. This suggests that these attacks are targeted rather than opportunistic, with attackers likely compromising networks for a period of time prior to executing the encryption routine to locate and exfiltrate sensitive data. ***As the cyber threat landscape continues to evolve to circumvent current security controls, the NTIC Cyber Center would like to emphasize the importance for***

organizations of all sizes to have a cyber incident response plan in place to effectively respond to a cyber attack. For more information on creating a cyber incident response plan for your organization, please download the NTIC Cyber Center Guide on Incident Response Planning.

Current and Emerging Cyber Threats

Phishing Campaign Disguised as a Password-Protected NortonLifelock Word Document

In January 2020, Palo Alto Unit 42 researchers discovered a phishing campaign featuring malicious Microsoft Word documents disguised as password-protected NortonLifelock documents. When users enter the correct access password, these malicious documents launch malicious batch scripts and execution files and deploy a remote access Trojan (RAT) called NetSupport Manager that grants attackers unlimited access to all system files. ***The NTIC advises administrators to implement effective email security controls, conduct regular security training for employees to help reduce risk and harden networks against email-based threats, and scan for and proactively block the indicators of compromise (IoCs) associated with this campaign.***

Android Banking Trojan Malware

ThreatFabric security researchers have detected an updated Android banking Trojan malware that now includes a remote access Trojan (RAT) that allows the threat actor to steal two factor authentication (2FA) codes by abusing Android accessibility privileges. This campaign targets one-time PIN codes sent viaSMS and forwards the codes to the attackers' server to be used to bypass 2FA. In addition, theRAT now has TeamViewer capabilities and gives full remote functionality to the threat actor to be able to change settings, unlock victims' phones remotely using screen-lock grabbing features, use apps on the device, and download content. ***The NTIC recommends network administrators and users reference and block the associated campaigns indicators of compromise (IoCs) by clicking here.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your

organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

PwndLocker Ransomware

Discovered in late 2019, PwndLocker ransomware, has recently been targeting local government and businesses with ransom demands ranging from $175,000 to over $660,000 depending on the size of the network. According to BleepingComputer, recent PwndLocker targets include Lasalle County in Illinois and the City of Novi Sad in Serbia. PwndLocker attempts to disable to multiple applications and services including security software. If successful, PwndLocker appends .key or .pwnd to the names of encrypted files and drops a ransom note named H0w_T0_Rec0very_Files.txt on infected systems. There are currently no known decryption tools available. More information about PwndLocker ransomware is available on BleepingComputer's website.

Romantic Nemty Ransomware Campaign

Threat actors are distributing Nemty Ransomware via emails that masquerade as correspondence from a romantic interest. These malicious emails feature subject lines such as "Don't tell anyone," "I love you," "Letter for you," "Will be our secret," and "Can't forget you." Included in the body of these email is a wink " ;) " text emoticon and a malicious ZIP archive payload. This campaign may slip past current security solutions as a malicious JavaScript file within the attached ZIP file is rated low on VirusTotal, making the malicious attachment difficult to detect. Additional information about Nemty ransomware, including decryption processes, is available on Bleeping Computer's website here.

Vulnerabilities

Broadcom and Cypress Wi-Fi Chips Vulnerability

Broadcom and Cypress Wi-Fi chips contain an encryption vulnerability named kr00k (CVE-2019-15126) that makes wireless packet communications sent via vulnerable devices susceptible to decryption. ESET researchers discovered this vulnerability in February and communicated its findings to Broadcom and Cypress who later published updates remediating the vulnerability in over one billion Wi-Fi capable devices and access points. ***The NTIC Cyber Center recommends keeping all Wi-Fi capable devices, including Wi-Fi access points and routers, up to date with the latest patches.***

Data Leaks and Breaches

Transmit Security, a Cybersecurity company with clients such as TD Bank and the First International Bank of Israel, disclosed a data breach affecting over one thousand client email addresses and phone numbers. According to a researcher, threat actors gained access to NextCloud, Transmit Security's file support-system. Transmit Security states that no passwords were compromised and no customer information from clients were affected. Transmit Security has since shut down its NextCloud system. ***The NTIC Cyber Center recommends readers remain vigilant for phishing emails and refrain from clicking on links from unknown or untrusted sources. We also recommend enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Insurance company Pacific Specialty reported that a phishing campaign targeting employee email accounts resulted in a breach of customer data. The company, which provides automotive and home insurance services in all US states, believes an unauthorized third party accessed the names, Social Security numbers, government-issued identification, financial, and other payment card information, and health insurance information of an unknown number of customers. ***Though the company has issued notifications to affected individuals, the NTIC Cyber Center encourages all Pacific Specialty customers to monitor their account statements and immediately notify their financial institutions of any suspicious or unauthorized activity. In addition, we advise customers to remain vigilant for a possible increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Facial-recognition and artificial intelligence company Clearview AI disclosed a data breach that resulted in the exposure of the company's client list. The company indicates that an unauthorized third party gained access to information that revealed Clearview AI's customers, comprised

primarily of law-enforcement agencies, as well as numbers of customer searches and user accounts. Client search histories are not believed to have been compromised in this breach. ***The NTIC Cyber Center advises law enforcement agencies to remain vigilant for a possible increase in phishing attempts perpetrated as a result of this data exposure.***

Privatized railroad track and transit system provider, Railworks, disclosed a ransomware incident that resulted in the compromise of data for current employees, former employees, beneficiaries, dependents, and contractors. Compromised information includes names, addresses, driver license numbers, government IDs, Social Security numbers, dates of birth, and dates of hire/termination/ retirement. Railworks has 45 offices in the United States and Canada with over 3,500 employees and holds multibillion dollar contracts with other railroad organizations and transit authorities. ***The NTIC Cyber Center encourages those affected to consider placing a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring services offered to affected personnel and enabling multifactor authentication (MFA) on all accounts that offer it.***

Upcoming Webinars

How Fortune 500 Companies Are Using Gamification To Change Behavior

It is human nature to enjoy reward, recognition, and progress. Cybersecurity gamification embraces these motivational triggers to encourage even the biggest stragglers to be in it to win it. A Pulse Learning Study found 75 percent of respondents indicated they would be more engaged if learning involved gaming dynamics. Gabe Zichermann, world's foremost expert and public speaker on the subject of gamification, user engagement and behavioral design and the co-founder of the behavior change software startup, Onward, and Masha Sedova, Co-founder of Elevate Security and award-

winning cybersecurity expert, will share cybersecurity secrets on how enterprises are using gamification as a strategy to influence better cybersecurity behaviors.

To register for this free webinar on Thursday, March 5 at 11:00 AM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Whether tax season elicits delight or dread, one thing is for sure: it's prime time for scammers to perpetrate **Internal Revenue Service (IRS) tax scams**. These scams may come in a variety of forms, all designed to separate you from your money. Click here to read more about this prevalent scam and learn how to protect yourself

---

Cyber in the News

Scammers Take Advantage of COVID-19 Outbreak to Carry Out Fraud
Analytic Comment: Scammers are using news related to the COVID-19 outbreak to perpetrate fraudulent activity via the Internet, social media networks, and email. One such example is "pump-and-dump" stock schemes, whereby scammers encourage others to invest in a company affiliated with preventing, detecting, or curing COVID-19, only to cash in on the artificial inflation of the stock's price that ensues. Scammers have also used COVID-19-themed websites and emails to sell counterfeit products, steal personal information, and distribute malware. Such schemes underscore the importance of remaining vigilant for fraudulent websites, social media pleas, or phishing emails exploiting the COVID-19 outbreak. For additional information on fraudulent activity surrounding similar events, see the NTIC Cyber Center's blog posts on disaster scams and charity scams.

For better election security, get to know the IT people

Analytic Comment: In response to the upsurge of cyber attacks across the nation, the National Governors Association (NGA) is urging Congress to pass legislation for more grant funding for states and local municipalities. A recent report by security firm Emsisoft estimated that ransomware affected at least 966 government entities, educational institutions, and healthcare providers last year. Furthermore, according to the Research and Technology Subcommittee, the lack of skills and education contribute to vacant cybersecurity positions. This underscores the importance of proper cybersecurity related funding so that vulnerable organizations may pay for properly trained personnel.

Patches and Updates

Cisco Releases Security Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Emerson ValveLink

Moxa AWK-3131A Series Industrial AP/Bridge/Client

Omron PLC CJ Series

PHOENIX CONTACT Emalytics Controller ILC

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-03-018

HSEC-1 | NTIC SIN No. 2.5, 5.4

March 12, 2020

National Capital Region Cyber Threat Spotlight

Online Coronavirus Scams

Amazon and other online retailers have removed over one million listings associated with products that are in high demand as a result of the recent COVID-19 outbreak, citing fraudulent claims and price-gouging from third party vendors. According to the cybersecurity firm Proofpoint, the Wall Street Journal has reported that the number of emails containing the word "coronavirus" has skyrocketed in recent weeks, with malicious emails appearing to come from reputable organizations. The Better Business Bureau (BBB) recommends consumers maintain awareness of face mask scams selling counterfeit or low-quality masks that do not offer adequate protection against the COVID-19 virus. These fraudulent websites collect payments and personal information, but either provide consumers with low-quality or counterfeit goods, or do not deliver anything at all. ***The NTIC Cyber Center recommends making purchases of these types of items through CDC-approved vendors to guarantee quality and delivery of supplies while maintaining awareness of the potential for***

malicious actors to spoof legitimate websites, send malicious emails, and generate fraudulent billing requests.

Current and Emerging Cyber Threats

Malicious Code Embedded in Fraudulent Coronavirus-Related Websites

Security researchers at MalwareBytes labs discovered malicious code embedded in a website that hosts a fraudulent copy of Johns Hopkins University's interactive COVID-19 heatmap. The website, registered in February 2020 using Russian nameservers, is infected with a variant of AzorUlt spyware that is capable of skimming visitors' passwords and payment card details as well as deploying other malware. Since there are no indications that the website has been used in malicious email campaigns, researchers believe the threat actors have relied on organic visitor traffic to the website to propagate the information-stealing malware. ***The NTIC Cyber Center advises web users to remain vigilant for fraudulent websites, social media pleas, or phishing emails exploiting the COVID-19 outbreak. In addition, we advise those seeking to reference Johns Hopkins University's legitimate COVID-19 map to do so only using the official link, found here. For additional information on fraudulent activity surrounding similar events, see the NTIC Cyber Center's blog posts on disaster scams and charity scams.***

GuLoader Malware Uses Cloud Services to Store Malicious Payload

In late December 2019, Proofpoint researchers discovered a new malicious downloader that has been dubbed "GuLoader" and is a portable executable file, written partially in Visual Basic 6.0, used to deliver Parallax RAT, a remote access Trojan used to gain control of infected systems. GuLoader stores its encrypted payloads on cloud services such as Google Drive and Microsoft One Drive to bypass restrictions on networks. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and running reputable and up-to-date antivirus software. We encourage network administrators to block all associated indicators of compromise (IoCs) provided in Proofpoint's report.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide

important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

PwndLocker

Emsisoft has discovered a way to decrypt files encrypted by PwndLocker ransomware, allowing victims of these attacks to recover their data without having to pay the demanded ransom. To begin the decryption process, Emsisoft requires only a copy of the ransomware's executable file that was used in the attack. Although threat actors usually delete this executable file during a ransomware attack, Emsisoft advises victims to recover the file using Shadow Explorer or other file recovery tools.

Ryuk Ransomware Impacts eDiscovery Firm

Epiq Global, an eDiscovery and legal services firm, recently disclosed that a ransomware attack compromised the company's systems. The ransomware affected their eDiscovery platforms, hindering clients from accessing needed legal documents. A source reported to BleepingComputer that an initial Trickbot banking Trojan infection was responsible for ultimately distributing Ryuk ransomware to the company's systems. Epiq Global took their systems offline to contain the threat and has since engaged a third-party forensic firm and law enforcement authorities to investigate the incident.

Cloud Storage Backups Compromised with Ransomware

DoppelPaymer and Maze ransomware operators have started to compromise cloud storage backups. While backups are extremely important for ransomware mitigation, improper configuration can render them useless in a ransomware attack. Threat actors conducting DoppelPaymer attacks have published credentials associated with victims' backup software on publicly viewable websites in order to alert victims of the compromise of their entire network including backups. Discovered and analyzed in mid-2019 by CrowdStrike researchers, DoppelPaymer ransomware shares code with both the BitPaymer ransomware variant and the Dridex banking Trojan and can both steal and encrypt data. While corresponding with members of the cybersecurity website BleepingComputer, the threat actors behind Maze ransomware campaigns claimed that that they leverage cloud storage backups to pilfer victims' data. The threat actors did not expound on methods used to obtain the cloud credentials.

Vulnerabilities

Apache Tomcat Web Application Server Vulnerability

A security firm discovered a vulnerability in Apache Tomcat, a web application server, dubbed Ghostcat (CVE-2020-1938) that allows threat actors to read and write files and potentially take over unpatched systems. Threat actors exploit the vulnerability by leveraging a flaw in the Tomcat Apache JServ Protocol (AJP) protocol that allows them to modify webapp directories within Tomcat. One report indicates that over one million Apache Tomcat servers exist online and could be vulnerable to this attack. This vulnerability affects all versions of Apache Tomcat and a patch is available. ***The NTIC Cyber Center recommends system administrators immediately upgrade Apache Tomcat to the latest version. If you believe your system has been compromised, notify your organization's IT security team immediately.***

Zoho ManageEngine Desktop Central

Cybersecurity researchers have discovered a zero-day exploit affecting Zoho ManageEngine Desktop Central that provides attackers an entry point to infect corporate networks with ransomware. Zoho ManageEngine Desktop Central is an endpoint management solution system used to control, remotely access, and send updates to groups of devices such as Android smartphones, Linux servers, or Mac and Windows workstations. The vulnerability allows threat actors to execute malicious code on the management server without being authenticated and could grant attackers full control of a company's fleet of devices to encrypt or steal data. Threat actors can also use this zero-day vulnerability to move laterally through an organization's network and push other types of malware to all users on that network. ***The NTIC Cyber Center recommends all administrators of Zoho ManageEngine Desktop Central update to the latest version 10.0.476 as soon as possible.***

Data Leaks and Breaches

J.CREW

Clothing retailer J.Crew announced that an unauthorized third party used a credential stuffing attack to gain access to customer accounts. Likely leveraging credentials stolen in another breach, the threat actor was able to log into targeted accounts and access consumer information including payment card type, the last four digits of payment cards, expiration dates, billing addresses, order numbers, and order shipment status. In response, J.Crew has disabled compromised accounts and requests customer verification and password resets for account reinstatement. ***The NTIC Cyber***

Center encourages the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.

For more information on credential stuffing attacks, please reference the NTIC Cyber Center's product entitled Credential Stuffing Attacks – A Growing Yet Easily Mitigated Threat.

Cellular phone carrier, T-Mobile, disclosed a data breach affecting its prepaid customers in which unknown threat actors gained unauthorized access to an undisclosed number of customer accounts via compromised T-Mobile employee email accounts. In some cases, breached data included customer Social Security numbers, government ID numbers, financial information, billing information, and rate plans. T-Mobile states that no passwords were compromised and that they will notify affected customers. ***The NTIC Cyber Center encourages those affected to consider placing a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring services offered to affected consumers, enabling multi-factor authentication (MFA) on all accounts that offer it, changing account PINs, and immediately notifying their financial institutions and T-Mobile customer service of any unauthorized or suspicious activity.***

Cruise ship operator, Carnival Corporation, disclosed a data breach affecting its guests in which unknown threat actors gained unauthorized access to an undisclosed number of customer accounts via compromised Carnival employee email accounts. In some cases, breached data included customer names, Social Security numbers, government ID numbers, financial information, and credit card information. Carnival states that there has been no evidence to suggest that the data has been misused and has reported the incident to law enforcement. ***The NTIC Cyber Center encourages those affected to consider placing a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring services offered to affected consumers, enabling multi-factor authentication (MFA) on all accounts that offer it, and immediately notifying their financial institutions and Carnival customer service of any unauthorized or suspicious activity.***

Pharmacy company Walgreens has disclosed a breach of data that exposed the personal and health-related information of an unknown number of customers who use the company's mobile application. The company's notification indicates that an error in the mobile application may have allowed some customers to view other customers' messages containing customer names, prescription numbers, drug names, store numbers, and shipping addresses. Walgreens has notified affected customers of the incident, which occurred between January 9 and January 15, 2020, and has remedied the errors in the mobile application that precipitated the data breach. ***The NTIC Cyber Center encourages users of the Walgreens mobile application to remain vigilant for a possible increase in phishing attempts perpetrated as a result of this data exposure.***

Upcoming Webinars

The Legal and Investigative Implications of Emojis

This webinar, presented by cyber crime attorneys and a former prosecutor, discusses investigative uses of emojis, particularly in the context of child exploitation, and the legal context of this growing medium, including current case law and implications for practice.

To register for this free webinar on Thursday, March 25 at 2:00 PM EST, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Have you ever seen a friend's social media post promoting a product at such an incredible discount, you almost couldn't resist clicking the advertisement and making a purchase? Not so fast! You may have encountered a **fake social media ad scam**. Click here to read more about this prevalent scam and learn how to protect yourself

---

Cyber in the News

Data-breach bill gives D.C. power to go after companies with weak cybersecurity

Analytic Comment: A new bill recently passed in Washington, DC has expanded the scope of information protected under the District's data breach laws. The bill adds personally identifiable information such as passport numbers, military identification, health and biometric data, and genetic profiles stored on genealogy websites to the list of information that must be disclosed in data breaches under the District's 2007 data breach notification law. The bill also gives the DC Office of the Attorney General more power to pursue legal action against entities whose weak cybersecurity measures result in the unauthorized disclosure of such information. Additionally, the bill requires companies that experience a breach to furnish detailed records of their data-protection measures and provide 18 months of free credit monitoring to any resident whose Social Security number is compromised in a breach. This bill positions the District's data breach laws as among the strongest in the US and should serve as a model for other states seeking to toughen their stance on data protections for consumers.

Counties need cyber disaster plans, too

Analytic Comment: Several attendees at the recent National Association of Counties conference in Washington, DC noted that the need for local governments to protect IT assets from cyber attacks is greater that ever before. With ransomware attacks increasingly targeting local and county governments and Internet-enabled devices proliferating and exposing more avenues for attacks, officials argue that governments must prepare for cyber disasters with emergency responses similar to those activated during physical disasters. In addition, local government officials recommend implementing a risk-based approach that prioritizes investments in cyber security to ensure protection against the costly loss of data or other impacts of cyber attacks to county infrastructure.

The Case for Limiting Your Browser Extensions

Analytic Comment: The website of a major healthcare company was recently flagged as serving malicious code after an employee of the company edited the website while using a browser configured with an infected browser extension. In this case, the browser extension was Page Ruler, an add-on to Chrome that allows users to measure the dimensions of images on a computer screen, and not only was it spreading malicious code, but it was also serving advertisements to website visitors. Security researchers warn that malicious browser extensions such as these are dangerous and could be configured with read and write access to all data on a compromised browser. This news underscores the importance for all Internet users to be cautious when installing browser extensions and avoiding extensions whose permissions requests don't match their functionality, declining requests from websites that push unwanted extensions, and ensuring that any extension downloaded comes from a legitimate source and publisher.

Patches and Updates

Cisco Releases Security Updates

Intel Releases Security Updates

Microsoft Releases March 2020 Security Updates

Mozilla Releases Security Updates for Firefox and Firefox ESR

Zoho Releases Security Update on ManageEngine Desktop Central

---

ICS-CERT Advisories

Johnson Controls Kantech EntraPass

Johnson Controls Metasys

Rockwell Automation MicroLogix Controllers and RSLogix 500 Software

Siemens PROFINET-IO Stack (Update A)

Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update A)

Siemens SIMATIC S7 (Update A)

Siemens SIMATIC S7-1500 (Update A)

Siemens SiNVR 3

Siemens Spectrum Power 5

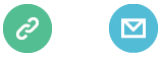
SIMATIC S7-300 CPUs and SINUMERIK Controller over Profinet

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-03-026

HSEC-1 | NTIC SIN No. 2.5, 5.4

March 19, 2020

National Capital Region Cyber Threat Spotlight

Local COVID-19 Scams

The Bowie Police Department is currently investigating reports of a man dressed in a black hoodie, orange vest, and blue surgical mask knocking on residents' doors claiming to be "inspecting for the COVID-19 virus." In one incident, the man left after the homeowner did not allow him inside. In a second incident, the man entered a home through an unlocked door and was confronted by the resident. The man fled after hearing a dog bark. Police are warning residents not to allow anyone claiming to be a COVID-19 inspector into their homes.

In another report, Maryland residents are receiving phone calls from scammers claiming to be representatives of local healthcare facilities and offering a cure for COVID-19 in exchange for the call recipient's credit card information. Police are warning residents not to provide credit card information during unsolicited calls and to take extra steps to verify callers.

The NTIC Cyber Center urges all members to maintain awareness of these and other scams associated with the COVID-19 pandemic and educate friends and family. If you or a loved one witnesses or becomes a victim of a COVID-19-related scam, please contact your local police department immediately.

Federal Partner Announcement

CISA Releases Alert on Enterprise VPN Security

As organizations prepare for possible impacts of Coronavirus Disease 2019 (COVID-19), many may consider alternate workplace options for their employees. Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network. As organizations elect to implement telework, the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity. For a list of recommended mitigation strategies, please see CISA Alert AA20-073A.

Current and Emerging Cyber Threats

Fraudulent COVID-19 Tracking Apps for Android Steal Data, Lock Devices

Researchers from security firm DomainTools noticed an increase in domains registered with names related to the COVID-19 pandemic leading to misleading websites equipped with maps and pertinent data to exploit concerned users. These websites contain links with instructions on how to download an Android application that promises to help track updates on the COVID-19 pandemic. However, if installed, this application will infect the victim's device with malware and attempt to steal data. This application falsely claims to be certified through the World Health Organization (WHO) and, upon installation, it requests various permissions including access to the victim's lock screen, giving attackers the ability to lock victims out of their devices and demand a ransom to regain access. ***The NTIC Cyber Center recommends all Android users remain vigilant for fraudulent, malicious apps posing as COVID-19 status trackers or any other apps associated with the pandemic and to thoroughly read user reviews and ratings to help determine the app's legitimacy. If the device permissions required by an app do not match the advertised functionality, refrain from installing it.***

BEC Schemes Exploit COVID-19 to Divert Payments

Researchers from cybersecurity firm Agari discovered a Business Email Compromise (BEC) scheme that exploits the COVID-19 pandemic to try and trick companies into diverting payments for outstanding invoices to attackers' accounts. Using financial aging reports, the threat actors behind this campaign impersonate a company's executives and request payment for the invoices

from the company's customers. The body of these emails include the following: "Due to the news of the Corona-virus disease (COVID-19) we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so i can forward you our updated payment information." ***The NTIC Cyber Center recommends maintaining awareness of this and other BEC schemes and scrutinizing any financial request that includes a change in normal, expected procedures. We highly recommend verifying all payment procedure changes with multiple people in your organization and contacting the sender via another means of communication, such as a direct phone call, to verify the legitimacy of the request.***

Cookiethief Android Malware Compromises Facebook Accounts

Security researchers have discovered a new Android malware family dubbed Cookiethief, that can take over a Facebook account. Once an Android device is infected, threat actors steal Facebook cookie data and initiate a proxy on the target device to make a spoofed login appear legitimate. Threat actors are then able to take over the Facebook account and distribute malicious content. It currently unknown how the threat actors initially compromise Android devices with Cookiethief. ***The NTIC Cyber Center recommends Android users keep device operating systems up-to-date and enable two-factor authentication on their accounts, and avoid reusing passwords across multiple platforms.***

Fake HIV Test Results Infect Victims with Koadic RAT

Researchers have recently discovered a spear phishing email campaign using HIV test results to lure victims into opening a malicious Microsoft Excel document that contains the Koadic remote access Trojan (RAT). The threat actors in this campaign imitate Vanderbilt University Medical Center sending emails with a subject line “Test result of medical analysis” and try to trick users into opening a file labeled *TestResults.xlsb*. Once victims open the file, they will be promoted to enable macros, launching the Koadic RAT and allowing the attackers control over the infected system. ***The NTIC Cyber Center recommends users remain vigilant for malspam or spear phishing campaigns disguised as healthcare correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your

data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Coronavirus Ransomware

Security researchers at MalwareHunterTeam have discovered a website that claims to offer downloads of the Windows system optimization tool WiseCleaner but instead distributes an information-stealing Trojan called Kpot and a new ransomware called CoronaVirus. The Kpot Trojan is capable of stealing cookies and login credentials from browsers, email accounts, messaging programs as well as taking screenshots of a user's desktop and stealing cryptocurrency wallets from infected systems. The CoronaVirus ransomware then encrypts a number of files on the targeted computer and demands a ransom of 0.008 Bitcoins (~$50 USD). As this cyber attack contains ransomware and information-stealing elements, users affected by this attack should use another computer to immediately change the passwords to all online services and accounts used on the infected computer, as these credentials have likely been compromised. The NTIC Cyber Center recommends administrators reference and proactively block the associated indicators of compromise (IoCs) found here.

Microsoft Warns of Human-Operated Ransomware Attacks

Microsoft warns that human-operated ransomware campaigns are a significant and growing threat. A threat actor's advanced expertise allows them to adapt in what they discover and compromise accounts with higher privileges, lateral movement, or use credential dumping techniques to compromise accounts unlike most automatic wormable threats such as WannaCry or NotPetya. Human-operated ransomware campaigns that include ransomware such as REvil, Samas, Bitpaymer, and Ryuk may also deliver various malicious payloads, steal credentials, and access and exfiltrate data from compromised networks. Network security professionals should take proactive steps to prevent and mitigate these attacks by implementing security policies and procedures to combat infrastructure weaknesses.

PXJ

Researchers from IBM's X-Force Incident Response and Intelligence Services (IRIS) discovered a new strain of ransomware now known as "PXJ" derived from the file extension that is appended to encrypt files and a second name "XVFXGW" based off the email addresses listed in the ransom note. The same as most ransomware, PXJ disables the victim's ability to recover any files from deleted stores or shadow copies while using a double encrypting technique on compromised data and then dropping a ransom note with the file name "LOOK.txt" on infected systems.

Paradise

Threat actors are embedding Paradise ransomware via malicious spam (malspam) campaigns that contain malware-laden attachments. First observed in 2017, Paradise uses RSA encryption to encrypt victim data and is known to be a Ransomware-as-a-Service (RaaS), a service that allows a low-skilled third-party to create and manage the ransomware campaign. In this current ransomware campaign, threat actors are sending emails that masquerade as offers, orders, or keys with an attach file in the .iqy format. The .iqy file can be used as a data source for an excel spreadsheet however threat actors can leverage it import data from remote URLs to launch unauthorized programs. More information about Paradise ransomware is available on Bleeping Computer's website here.

Vulnerabilities

WAGO

Researchers at Cisco Talos have identified numerous vulnerabilities in products made by electrical connection and automation solutions manufacturer WAGO. The vulnerabilities, which affect PCF100 and PCF200 programmable logic controllers and Touch Panel 600 HMI panels, could be exploited by attackers to execute arbitrary code, inject commands, steal information, facilitate denial of service (DoS) attacks, and take control of targeted devices. The NTIC Cyber Center advises administrators of environments containing WAGO devices to update devices to the latest firmware (version FW15 or above), consult US-CERT's advisory for mitigation strategies, and reference Talos's report for more information on these vulnerabilities.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Government grant scams are a type of social engineering scheme in which perpetrators use the promise of grant funding to steal money and/or elicit personally identifiable information (PII). Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

CIOs Face Challenges if Coronavirus Forces Government to Go Remote

Analytic Comment: State and local governments are facing mounting challenges in continuing to deliver critical public services while ensuring the health and safety of employees during the COVID-19 outbreak. Many governments are not currently outfitted with enough laptops and smartphones to give to employees working remotely, raising concerns that slow procurement and distribution processes of new equipment could hamper the delivery of critical public services. In addition, many agencies' work applications are not web-accessible, eliminating the possibility for employees to work remotely at all. These concerns should motivate state and local governments to ensure their incident response and continuity-of-operations plans are up-to-date and that their workforce is properly outfitted to sustain government functions, especially should the health crisis develop further.

Microsoft Orchestrates Coordinated Takedown of Necurs Botnet

Analytic Comment: Microsoft has announced the successful dismantling of the Necurs botnet, the global command and control (C&C) infrastructure that has directed over nine million infected computers worldwide to send malware-laced spam emails since 2012. The operation, completed in coordination with cybersecurity firms, Internet service providers, domain registrars, government entities, and law enforcement agencies across 35 countries, involved breaking the Necurs domain generation algorithm to predict which domain names the Necurs botnet would attempt to register next to host new C&C servers. Microsoft reports that they not only blocked all new Necurs C&C registrations, they have seized ownership of old C&C domains and are providing guidance to infected users on how to remove the malware from their computers. This effort represents one of the largest botnet takedown operations to date and should be praised as a much-needed response to controlling the spread of malware by email worldwide.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Enterprise VPN Security

Microsoft Releases Out-of-Band Security Updates for SMB RCE Vulnerability

VMware Releases Security Updates for Multiple Products

ICS-CERT Advisories

ABB Asset Suite

ABB eSOMS

Delta Electronics Industrial Automation CNCSoft ScreenEditor

Rockwell Automation Allen-Bradley Stratix 5950

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-03-035

HSEC-1 | NTIC SIN No. 2.5, 5.4

March 26, 2020

National Capital Region Cyber Threat Spotlight

COVID-19 Phishing Emails

Security researchers warn that attackers are using COVID-19 themed phishing emails and open redirect vulnerabilities to infect recipients with an information-stealing malware called Racoon. Open redirect vulnerabilities allow attackers to construct web addresses that appear legitimate but instead divert visitors to malicious destinations. In this campaign, attackers send phishing emails featuring carefully crafted links that abuse an open redirect vulnerability identified in a subdomain belonging to the US Department of Health and Human Services (HHS). When users click on the link, they are forwarded to a website that downloads and installs the Racoon malware, allowing attackers to steal information such as email credentials, credit card information, cryptocurrency wallets, browser data, and system information from almost 60 different software applications. Abuse of open redirect vulnerabilities adds legitimacy to spam emails and increases the likelihood that unsuspecting users will visit associated fraudulent login pages or other harmful websites. ***The NTIC Cyber Center advises email recipients to remain vigilant for malicious cyber activity exploiting the COVID-19 pandemic, beware of malicious links that redirect from other domains, avoid***

opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources.

For more information about open redirect vulnerabilities, including tips for web administrators on how to mitigate these risks, please see our Cyber Advisory entitled Open Redirect Vulnerabilities Facilitate Malicious Cyber Activity.

Federal Partner Announcement

FBI Warns Against COVID-19 Frauds

The FBI has identified a surge in COVID-19 related scams involving fraudulent Center for Disease Control and Prevention (CDC) emails, phishing emails, and counterfeit treatments or equipment all attempting to steal money or personal information from victims. These scams claim to provide pertinent COVID-19 information on charitable contributions, general financial relief (including economic stimulus checks), airline carrier refunds, fraudulent cures or vaccines, fake testing kits, and data tracking COVID-19 infections. You can locate counterfeit and unapproved Personal Protective Equipment (PPE) on the CDC website and report counterfeit products to the FBI's Internet Crime Complaint Center and to the National Intellectual Property Rights Coordination Center. For more information, please see the FBI's Public Service Announcement here.

Current and Emerging Cyber Threats

Phishing Emails Spoofing World Health Organization Deliver Hawkeye Malware

Security researchers have identified COVID-19-related phishing emails disguised as official correspondence from the Director-General of the World Health Organization (WHO). These emails

masquerade as informational resources for fighting COVID-19 but contain attached executable files that install the HawkEye malware to log victim's keystrokes, capture screenshots, steal user credentials from web browsers and email clients, and download additional malware. ***The NTIC Cyber Center reminds users and administrators to beware of phishing emails, social media pleas, or websites disguised as legitimate correspondence related to the COVID-19 pandemic. In addition, we encourage administrators to scan for and proactively block the indicators of compromise (IoCs) associated with this campaign*** *here.*

COVID-19 Email Extortion Scam

Sextortion scammers are adding the COVID-19 pandemic as a tool to scare and extort money from victims claiming they have victims' usernames and passwords and threatening to infect victims' families with the SARS-CoV-2 virus if the extortion demands are not met. This campaign sends emails with the subject "[YOUR NAME] : [YOUR PASSWORD]" as a tactic to get recipients to open the email and send $4,000 worth of Bitcoin to the attackers to prevent further harm. Despite these threats, it is important to note that the username and password combinations displayed in the email subject lines were likely obtained from recent data breaches and there have been no known cases where hackers have come in contact with targeted individuals or their family members to intentionally spread COVID-19. ***The NTIC Cyber Center urges all members to maintain awareness of these and other scams associated with the COVID-19 pandemic and educate friends and family. If you or a loved one witnesses or becomes a victim of a COVID-19-related scam, please contact your local police department immediately. For more information about these types of scams, please see our product titled*** *Securing Our Communities: Sextortion Scams****.***

Malicious Fraudulent COVID-19 Websites

Researchers have recently discovered websites that masquerade as COVID-19 antivirus protection while infecting unsuspecting victims with the BlackNET remote access Trojan (RAT). The threat actors built two websites that claim to battle COVID-19 with artificial intelligence developed by Harvard University scientists and urges visitors to download their application. Once victims download the malicious payload, BlackNET will infect the target system allowing the attackers control over the infected system. ***The NTIC Cyber Center recommends users remain vigilant for fraudulent sites advertising COVID-19 antivirus protection, keep legitimate antivirus applications updated with the latest virus definitions, and only download applications from trusted and vetted sources. If you believe your system has been compromised, notify your organization's IT security team immediately.***

New Cyber-Attacks on DNS Settings within Routers

Researchers discovered a new cyber-attack that hijacks the DNS settings on routers and displays browser alerts to prompt victims into downloading a fraudulent COVID-19 information application called “Emergency - COVID-19 Informator” or “COVID-19 Inform App” that claims to be from the World Health Organization (WHO). However, these malicious applications contain the Oski Trojan that, once installed, will steal victims’ browser cookies, browser history, payment information, saved login credentials, cryptocurrency wallets, Authy 2FA authenticator databases, among other information. This data is then uploaded to a remote server to be used to further compromise victims at a later time. ***Although it is not yet known how attackers are gaining access to routers to change the DNS settings, the NTIC Cyber Center recommends that all router owners and administrators disable remote administration on the router and change any default router login credentials as a precautionary measure. More information about how to fix affected routers is available on Bleeping Computer’s website.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Ransomware Threat Actors Claim They Will Not Target Healthcare Providers

Reports recently surfaced that the criminals behind various ransomware campaigns have pledged to stop targeting healthcare and medical organizations during the COVID-19 pandemic. According to a Bleeping Computer article, the operators of the Maze, DoppelPaymer, and NetWalker ransomware campaigns claimed that they either do not purposely target organizations within the healthcare sector or they would stop all “activity” against such organizations until the end of the pandemic. However, on March 14, Maze ransomware operators attacked UK-based Hammersmith Medicines Research and subsequently published sensitive data of the company’s former patients after the ransom demand was not met. Although some cyber threat actors may claim that they will cease destructive and disruptive attacks against certain sectors and organizations during the COVID-19 pandemic, the NTIC Cyber Center would like to remind our readers that there is no honor among thieves and that criminals, by nature, are untrustworthy, regardless of their claims. Fortunately, there are some “good guys” in this fight, as cybersecurity firms Emsisoft and Coveware announced that

they will offer ransomware decryption and negotiation services for free to healthcare organizations during the pandemic.

Delay in Ransomware Execution May Help Organizations Contain the Threat before Data is Encrypted

According to cybersecurity firm FireEye, threat actors deploy ransomware three days after the initial breach in 75 percent of all ransomware incidents. Threat actors tend to initially pilfer administrator credentials and exfiltrate victim's data before executing ransomware payloads. Stolen data can be used for leverage, such as threatening to publicly release it when victims do not remit payment. Some ransomware operators are much quicker in deploying ransomware as seen in prior GandCrab and GlobeImposter campaigns. Threat actors also tend to encrypt data outside of typical business hours to evade detection by the target organization's security team. While proactive measures are often the best way to mitigate incidents, there may still be a short window of opportunity after an initial breach to contain and remediate the threat before ransomware encrypts an organization’s data.

Nefilim

A new ransomware dubbed Nefilim shares similar code to Nemty ransomware. First observed in February 2020, Nefilim uses email correspondence for payment instead of Tor payment portals and is not offered as a Ransomware-as-a-Service (RaaS), a service that allows a low-skilled third-party to create and manage the ransomware campaign. Its threat actors and distribution method is currently unknown. In the Nefilim ransom note, threat actors state that they will publish stolen data from victims who do not remit payment in seven days. Once a target network is compromised with Nefilim, it will encrypt files using AES-128 encryption and will append .NEFILIM extension to file names. More information about Nefilim ransomware is available on Bleeping Computer’s website here.

Vulnerabilities

Remote Code Execution Vulnerability within Microsoft Adobe Type Manager Library

Microsoft has issued a security advisory on a remote code execution vulnerability that allows threat actors to take control of a compromised system. The vulnerability affects multiple Window versions and is rated "critical" depending on the version. The vulnerability is attributed to how Windows manages fonts from the Adobe Type Manager Library. If exploited, threat actors could prompt victims to view a malicious document, even through the Windows Preview pane. Microsoft has come up with several workarounds until a patch is a released. ***The NTIC Cyber Center recommends system administrators immediately use the Microsoft-provided workarounds and patch systems if***

and when a patch becomes available. If you believe your system has been compromised, notify your organization's IT security team immediately.

Data Leaks and Breaches

General Electric (GE)

General Electric (GE) disclosed that a breach of a third-party service provider resulted in the exposure of personal information belonging to current and former GE employees and their beneficiaries. According to GE's notification, an unauthorized individual gained access to an email account belonging to an employee of service provider Canon Business Process Services that contained sensitive GE employee documents. Data exposed in the breach includes names, addresses, Social Security numbers, driver's license numbers, bank account numbers, passport numbers, dates of birth, direct deposit forms, birth certificates, marriage certificates, death certificates, medical child support orders, tax withholding forms, beneficiary designation forms and applications for benefits such as retirement, severance and death benefits with related forms and documents, and other information. ***The NTIC Cyber Center recommends affected individuals remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. In addition, we encourage affected individuals to place a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. For more information about this incident and to register for credit monitoring and identity protection services, contact GE's support hotline at 1-800-432-3450 between 9 AM and 5 PM ET, Monday through Friday.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Counterfeit goods are fraudulent products that are similar or nearly identical to their legitimate counterparts and are typically sold for financial gain. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

COVID-19 Vaccine Test Center Hit by Cyber Attack, Stolen Data Posted Online

Analytic Comment: Cyber threat actors behind Maze ransomware have published data stolen in a recent ransomware attack on a British vaccine testing facility despite pledging to cease attacks on healthcare and medical sector targets during the COVID-19 pandemic. The ransomware operators have published samples of the stolen data, which allegedly include patient records belonging to individuals who underwent testing at the facility in the past, on the dark web to encourage the affected facility to pay the ransom. Security professionals fear that the ransomware group will continue to leak more of the data, eventually publishing it for all to see and use, should the organization not remit payment. This ruthless extortion of a critical facility underscores the fact that financial gain outweighs altruism as a primary motivator for many cyber threat actors and should serve as a reminder for all organizations to ensure proper mitigation strategies are in place to protect against ransomware and other cyber attacks, especially during this difficult time.

Coronavirus Cybercrime Task Force Launches in Virginia

Analytic Comment: The US Justice Department and the Commonwealth of Virginia have partnered to establish the Virginia Coronavirus Fraud Task Force to protect Virginia residents from fraudulent activities surrounding the COVID-19 pandemic. The task force's creation follows the US Attorney General's order to prioritize the prosecution of cybercriminals who seek to exploit the crisis. Among the fraudulent activities the task force will investigate are phishing campaigns, the impersonation of health officials or charities, the spread of malware, the theft of information, and others. The establishment of the Virginia Coronavirus Fraud Task Force, and the necessity out of which it grows, reinforces the need to maintain vigilance for cyber threats that may seek to capitalize on the public health crisis and illustrates the importance of including a cyber threat analysis component within the context of an all-threats response to the COVID-19 pandemic.

Justice Dept. Files Its First Coronavirus Takedown: A Bogus Vaccine Website

Analytic Comment: The US Department of Justice (DOJ) took action against its first COVID-19 fraud case in which a threat actor used a website to advertise the distribution of fraudulent vaccine kits from the World Health Organization (WHO). In reality, a vaccine for the COVID-19 virus does not currently exist. The website requested customer credit card information and a $4.95 shipping charge. The DOJ states that the website operators were conducting a wire fraud scheme that attempted to profit from people's confusion and fear due to the pandemic. The site has since been taken offline. This underscores the importance of remaining vigilant for scams during a time of crisis and disaster as threat actors will exploit public panic and desperation for profit.

Patches and Updates

Adobe Releases Security Update for Creative Cloud Desktop Application

Apple Releases Security Updates

Cisco Releases Security Updates for SD-WAN Solution Software

Drupal Releases Security Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Insulet Omnipod

Systech NDS-5000 Terminal Server

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-04-002

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 2, 2020

National Capital Region Cyber Threat Spotlight

Zoom Users at High Risk of Exploitation

Several reports have recently highlighted various cyber risks associated with the use of the video conferencing software Zoom. On March 30, the FBI published a press release warning Zoom users of "Zoom-bombing," an online attack in which unauthorized individuals access a video conference with the intent to shock legitimate Zoom users or disrupt the session by shouting profanities or displaying disturbing and inappropriate content. In another type of Zoom attack, security researchers discovered that attackers can steal Windows login credentials by embedding malicious links into Zoom's Group Chat feature. Additionally, a former NSA hacker just released two new zero-day vulnerabilities impacting Zoom software installed on a system running MacOS. The first vulnerability requires an attacker to have physical access to the device, but it allows the attacker to gain and maintain high-level user privileges for further exploitation. The second vulnerability exploits Zoom's access to a MacOS device's microphone and webcam. Lastly, a report from cybersecurity firm Check Point states there has been a major increase in the registrations of new domain names that include the word "zoom," many of which will likely be used as phishing sites or to deliver malware to unsuspecting victims. The company also detected a number of malicious executable files containing at least one instance of the word "zoom" in the file name, suggesting that threat actors may be trying to trick users into thinking that the malicious files are legitimate Zoom installation files or add-ons.

To reduce the risk of Zoom exploitation, the NTIC Cyber Center recommends the following:

- Set and require all users to input a "meeting password" for all Zoom video conferences.
- Enable the "waiting room" feature to prevent unauthorized users from entering an online meeting without the host's authorization.
- Restrict screen-sharing privileges to the host only.
- Never share your "Personal Meeting ID" with anyone.
- Lock online meetings after all authorized participants have joined.
- Do not post links to your meetings in a public forum and never upload screenshots of meetings to websites or social media platforms as you could inadvertently reveal sensitive information such as participants' names or Zoom meeting ID numbers.
- Make sure you are running the most up-to-date version of Zoom and only download Zoom software from the legitimate Zoom website: Zoom.us.
- Remember that Zoom does not currently provide end-to-end encrypted communications and anything said or displayed during a Zoom video conference could be recorded and shared with others. Refrain from sharing sensitive or classified information via the platform.

SMBs Targeted with Remcos RAT

Threat actors are attempting to infect small to medium-sized businesses (SMBs) with the Remcos remote access Trojan (RAT) via phishing emails masquerading as US Small Business Administration (SBA) correspondence. SMBs are experiencing financial hardships due to the current pandemic and threat actors are trying to trick them into downloading malware by using official-looking email correspondence disguised as disaster assistance grants and testing center vouchers. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as SBA correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign or infected with the Remcos Trojan, notify your organization's IT security team immediately.***

Current and Emerging Cyber Threats

WordPress Malware Distributed via Pirated Coronavirus Plugins

The same threat actors behind the WordPress WP-VCD malware are distributing pirated Coronavirus-themed plugin variants to insert backdoors to websites. These plugins inject malicious code into currently installed WordPress themes or various PHP files. Once the malicious plugin is installed on a WordPress site, it will attempt to compromise other sites on the same shared host and will regularly correspond with the attacker's command-and-control (C2) server and wait for new instructions. Threat actors are using these malicious plugins to generate income via popups or redirectors. ***The NTIC Cyber Center recommends WordPress website administrators avoid downloading plugins from unknown or untrusted sources, enable two-factor authentication on website administrator accounts, and properly vet all plugins prior to and after installation.***

Compromised Websites Deliver Malware Disguised as Chrome Updates

Compromised corporate sites and news blogs using the WordPress Content Management System (CMS) are being injected with a malicious JavaScript code to redirect visitors to phishing sites that deliver backdoor malware disguised as an update for Google Chrome. Once this malware is downloaded, it will install TeamViewer software giving the threat actor remote control of the compromised computer and deploy a second stage payload to the victim's computer with keyloggers, information-stealing malware, and other Trojans. These threat actors use geolocation and browser detection to target Chrome users from the United States, Canada, Australia, the UK, Israel, and Turkey. ***The NTIC Cyber Center recommends never downloading software or browser updates from unofficial sources, maintain awareness of legitimate websites that redirect users to unexpected websites, and to keep antivirus software updated with the latest virus definitions.***

BadUSB Attack Targets US Hospitality Provider

Researchers are investigating a rare attack on a US hospitality provider in which a threat actor mailed a fraudulent $50 Best Buy gift card to the company, along with a USB thumb drive supposedly containing an access list of items the recipient could purchase using the card. This attack, dubbed "BadUSB," attempts to trick victims into installing malware as, once inserted into a computer, the USB emulates keypresses to launch various automated attacks such as PowerShell commands designed to collect data from the system and send it back to the attacker. The threat actors behind this campaign and the malware used in the attack are currently unknown, but researchers suspect that it could be associated with the global cyber criminal group FIN7 known for targeting the hospitality and retail sectors since 2015. ***The NTIC Cyber Center recommends never***

inserting or mounting any unfamiliar storage devices or peripheral devices to systems and to report any suspicious and unsolicited packages containing such devices to your local police department and to the FBI's Internet Crime Complaint Center.

WordPress Plugin Vulnerability Provides Admin Privileges to Attackers

Security researchers warn that a vulnerability identified in the WordPress plugin "Rank Math" could allow attackers to gain administrative privileges on unpatched websites. In addition, a second vulnerability identified in the plugin could allow attackers to redirect visitors from any location on the site to other destinations. Researchers believe up to 200,000 WordPress sites may currently be at risk of attack as a result of these vulnerabilities. ***The NTIC Cyber Center encourages administrators of WordPress websites that have the Rank Math plugin installed to immediately upgrade to the latest version, 1.0.41.2, and maintain regular website backups that are stored securely off the network.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Ransomware Operators Create Websites to Publish Stolen Data

An increasing number of ransomware campaigns have begun threatening to publish victims' sensitive data to coerce them into paying the ransom. The threat actors behind the Nefilim, CLOP, and Sekhmet ransomware campaigns have each built separate websites to publish stolen information obtained from their victims. The threat actors behind the Maze ransomware first started this trend and then those behind the Sodinokibi/REvil, Nemty, and DoppelPaymer ransomware campaigns adopted the same tactics. It is important to note that, even if victims do pay the ransom, there is never any guarantee that the attackers will not sell or publicly release the data at a later time.

Vulnerabilities

HPE Solid-State Drives

Hewlett Packard Enterprise (HPE) notified their customers of a bug that will render their solid-state drives (SSD) obsolete after 40,000 hours of operation unless critical patch is applied. The bug affects versions older than HPD7 for specific models. The bug is attributed to the firmware and, once the point of failure is reached, the drive and data are unrecoverable. There are no known cases of threat actors exploiting this bug. This bug may reside with drives from other manufactures as well. ***The NTIC Cyber Center recommends system administrators immediately patch affected systems. More information about the bug and affected systems is available on HPE's advisory.***

Data Leaks and Breaches

The Maze ransomware group has allegedly conducted a ransomware attack against Chubb Group Holdings, Inc. a company that provides cybersecurity insurance. The attackers claim to have stolen personally identifiable information and threatens to release it if the ransom demands are not met. Chubb Group Holdings says there is no evidence that its own network has been breached and will be investigating a potential breach of a third-party provider. The Maze ransomware group has been actively targeting organizations across several sectors, including the healthcare sector. ***The NTIC Cyber Center encourages all organizations maintain current data backups that are stored securely off the network, regularly audit third-party access to networks, and audit networks for unauthorized access and exposed ports, especially those that are used for remote access such as TCP port 3389. For a list of recommended strategies to reduce the risk of becoming a victim of a ransomware attack, please download the NTIC Cyber Center Ransomware Mitigation Guide.***

Marriott disclosed a data breach that resulted in the exposure of personal information for approximate 5.2 million hotel guests. According to Marriott's notification, they noticed an

unauthorized third party accessing data at the end of February 2020 via compromised employee credentials. Marriot believes that the threat actor may have started accessing systems mid-January 2020 and is currently conducting an investigation. Information exposed in the data breach includes customers' names, dates of birth, genders, mailing addresses, e-mail addresses, and loyalty account numbers. Marriott does not currently believe data associated with their Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers have been involved. ***The NTIC Cyber Center encourages those affected to place a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring and identity protection services offered to affected customers. For questions or concerns, please call Marriott's dedicated service line at 1-800-598-9655***.

Tupperware®

Home products company Tupperware acknowledged a breach of customer data from their ecommerce website as a result of Magecart payment skimming attacks. By infecting the company's website with malicious code, attackers were able to steal names, addresses, email addresses, phone numbers, and payment card information from any US or Canadian visitor who entered the data on tupperware.com between roughly March 20, 2020 and March 25, 2020. Security researchers at MalwareBytes notified Tupperware, who removed the skimming code from the website and is currently investigating the incident. ***The NTIC Cyber Center recommends that customers who may have made purchases through Tupperware's ecommerce website during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Upcoming Webinars

DRAGOS

Ransomware in an Industrial World

Ransomware has become one of the most common methods of profit for cybercriminals – and a major cause of disruption. And it has the power to attack all industries indiscriminately. In light of

recent events demonstrating the concerns around industrial control systems and untargeted ransomware, this webinar will tackle the topic head-on.

Join Jason Christopher and Dave Bittner as they share their thoughts on trends and strategies associated with this new cyber risk.

They'll cover:

- The uniqueness in ICS environments, compared to traditional IT systems, and what that means for ransomware
- What we've learned from recent ransomware attacks
- The importance of knowing your systems—not just the protections in place—when managing cyber risk

To register for this free webinar on Thursday, April 2 at 1:00 PM EDT, click here

---

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Payroll diversion scams, also known as direct deposit diversions, are social engineering scams in which perpetrators send deceptive emails to human resources or finance departments to divert direct deposit payments to a bank account they control. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

New York Launches IT "SWAT Teams" to Aid Pandemic Response
Analytic Comment: The New York State Office of Information Technology Services has begun recruiting non-governmental IT professionals to aid with the state's IT needs during the COVID-19 pandemic. These groups, called "COVID-19 Technology SWAT Teams," will support IT efforts across the state to expand the digital infrastructure for facilitating COVID-19 testing, improve residents' access to state service, deliver public health guidance, and provide IT support to current

and new hospital facilities. This industry-government collaboration should provide a model for states seeking to tackle questions surrounding the COVID-19 public health crisis in the challenging weeks ahead.

Widely Available ICS Attack Tools Lower the Barrier for Attackers

Analytic Comment: According to security researchers at FireEye, the increasing availability of industrial control system (ICS) cyber attack tools has lowered the barriers of entry for attackers seeking to target ICS networks and systems. While ICS cyber attacks were previously reserved for those with specialized knowledge and skillsets, the proliferation of tools now grants low-level cyber threat actors the ability to target a variety of systems from manufacturers such as Advantech, Schneider Electric, Siemens, Cogent, GE, and many others. The widespread availability of these tools should serve as an indicator of the evolution of the threat landscape facing ICS systems and should encourage administrators to secure their systems against threats, not only from seasoned experts, but from unsophisticated actors as well.

FBI Turns to Insurers to Grasp the Full Reach of Ransomware

Analytic Comment: The Federal Bureau of Investigation (FBI) is taking steps to ensure victims of ransomware continue to report instances of infections. In recent meetings, FBI officials met with insurance industry representatives to collaborate on efforts to stop ransomware. Discussion topics included the frequency of ransomware events, which businesses are most at risk, the specifics of extortion demands, and defensive strategies to fend off emerging attack techniques. The value of these public-private collaborations serves to fill intelligence gaps in the mission to defend against costly and destructive ransomware attacks.

Patches and Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Advantech WebAccess

BD Pyxis MedStation and Pyxis Anesthesia (PAS) ES System

Hirschmann Automation and Control HiOS and HiSecOS Products

Mitsubishi Electric MELSEC

Schneider Electric IGSS SCADA Software

Schneider Electric Modicon Controllers (Update A)

VISAM Automation Base (VBASE)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

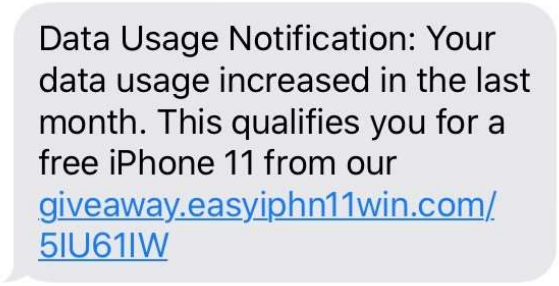
Product No. 2020-04-012

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 9, 2020

National Capital Region Cyber Threat Spotlight

SMS Scam Promises Free iPhone 11



A member of the NTIC Cyber Center recently received an SMS message (seen above) that attempts to trick recipients into believing that they are eligible for a new iPhone 11 as a result of an increase in cellular data usage. Although the URL included in this SMS message no longer resolves to a website, WHOIS records indicate that it is a newly registered domain name and is associated with the IP address 192[.]64[.]114[.]140. Open source research conducted on this IP address reveals its association with other potentially malicious campaigns. ***The NTIC Cyber Center recommends never clicking on links embedded in unexpected SMS messages or SMS messages from unknown senders.***

Federal Partner Announcement

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the United Kingdom's National Cyber Security Centre, released an alert to provide information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the the current coronavirus disease 2019 (COVID-19) global pandemic. This alert includes a non-exhaustive list of indicators of compromise (IoCs) for detection as well as mitigation advice. ***The NTIC Cyber Center recommends all network administrators review CISA Alert AA20-099A COVID-19 Exploited by Malicious Cyber Actors and proactively blocking the associated IoCs.***

Current and Emerging Cyber Threats

Office 365 Phishing Campaign Uses CSS to Bypass Security

Unknown threat actors have devised a malicious email campaign that steals credentials or infects systems via spoofed Office 365 voicemail notification emails. Threat actors leverage Cascading Style Sheets (CSS) to modify text in different languages so that backwards text appears normal to recipients and allows for malicious content to bypass secure email gateways. ***The NTIC Cyber Center recommends users remain vigilant for malicious email campaigns disguised as Office 365 correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources.***

MSSQL Servers Targeted in Cryptomining Campaign

Researchers at Guardicore Labs discovered an ongoing brute force campaign targeting Microsoft SQL (MSSQL) servers with weak credentials, infecting between 2,00 and 3,000 servers daily with cryptominers, remote access trojans (RATs) and a wide range of other malware. Researchers investigating this campaign have dubbed it Vollgar, because the crypomining scripts deployed on compromised servers will mine for both Monero and Vollar cryptocurrencies. Approximately 120 IP addresses have been linked to this campaign with most coming from previously compromised MSSQL servers in China. This campaign uses a wide range of malicious capabilities through the command-and-control (C2) platform by downloading files, installing Windows services, and running keyloggers with screen capture capabilities, activating the compromised server's webcam or

microphone and using the infected servers to launch DDoS attacks. Vollgar has been proven to bypass remediations like antivirus and EDR products, installing several backdoors to remain persistent. ***The NTIC Cyber Center recommends MSSQL server administrators enforce strong password policies, avoid exposing MSSQL servers to the internet, and create segmentation and whitelist access policies. Administrators should regularly audit MSSQL servers for suspicious and unexpected login attempts.***

LimeRAT Malware Campaign Exploits Excel Default Password

Mimecast researchers have observed an increase in LimeRAT malware campaigns using Microsoft Excel's "VelvetSweatshop" default password for delivery. These threat actors create an Excel read-only file to encrypt the file without needing to create an external password, making it easier to trick unsuspecting victims into opening the file and installing the malware. This Excel spreadsheet is delivered through a phishing scheme that lures unsuspecting victims into installing LimeRAT, giving the hacker the control to deliver ransomware, cryptominers, keyloggers, or to turn the victim's computer into a bot client. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization's IT security team immediately.***

BEC Scams Change Tactics Due to Pandemic

Threat actors conducting business email compromise (BEC) scams that masquerade as trusted officials and use victims to launder money via gift cards have changed their tactics to adapt to the current pandemic. Since customer traffic at physical stores has decreased, threat actors are now requesting digital gift cards from victims. Threat actors may request that victims communicate with them through unofficial communication platforms such as SMS to bypass email security. ***The NTIC Cyber Center recommends maintaining awareness of BEC schemes and scrutinizing any financial request that includes a change in normal, expected procedures. We highly recommend verifying all financial transaction procedures with multiple people in your organization and contacting the sender via official communication channels, such as a direct phone call, to verify the legitimacy of the request.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Ransomware Targets Biotech Firm

10x Genomics Inc., a biotech firm that produces coronavirus research tools, disclosed an attempted ransomware attack on their systems that occurred in March. The attack also included the theft of certain company data as well. Since then 10x Genomics Inc. has restored operations to its normal state and is working with third-party consultants and law enforcement for further investigation.

Vulnerabilities

HP Support Assistant

Several critical vulnerabilities have been found within HP Support Assistant for Windows OS, exposing systems to remote code execution attacks. HP Support Assistant has come pre-installed on HP desktops and notebooks since October 2012 and is used to facilitate automated updates and support. Threat actors will typically leverage this vulnerability during later attack phases to escalate privileges and maintain persistence. ***The NTIC Cyber Center recommends affected Windows users monitor systems for unusual and suspicious activity and update HP Support Assistant if and when a patch becomes available.***

Data Leaks and Breaches

Researchers at vpnMentor discovered a breach of data belonging to 14 million users of the loyalty and membership card application, Key Ring. Information exposed includes membership cards

details, government IDs, medical ID cards, and credit cards details. Additionally, 44 million images uploaded by Key Ring users were also exposed. The breach is attributed to improperly secured Amazon Web Services (AWS) S3 buckets, leaving them publicly exposed for anyone to access. The AWS buckets have since then been secured, although it is unknown if any threat actors abused the exposed data before then. ***The NTIC Cyber Center recommends Key Ring customers and associates remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. We also recommend Key Ring users monitor associated payment accounts and report any suspicious and unauthorized activity to their financial institutions.***

Upcoming Webinars

DRAGOS

Leveraging Managed Threat Hunting for an Effective ICS/OT Cybersecurity Program

Managed Detection and Response and Managed Threat Hunting solutions have been available for the Enterprise IT networks for many years but have been lacking in ICS/OT. Until now.

Dragos is launching the first MTH program for ICS/OT called Neighborhood Watch.

Join Tim Conway and Robert M. Lee for a discussion about the value of MDR/MTH programs, considerations to keep in mind and how to evaluate offerings. Youll learn about:

- Providing more security coverage with fewer staff resources
- Transferring knowledge to your cybersecurity staff team for long term success
- Identifying threats often leveraging a vendor's technology stack
- Evaluating cost, time to ramp and overall effectiveness

To register for this free webinar on Friday, April 17 at 1:00 PM EDT, click here

Enhancing Your Teleworkers' Cybersecurity During the COVID-19 Pandemic

Tens of millions are now teleworking due to the coronavirus. This has happened suddenly and with little notice. If you are a cybersecurity leader in government or industry, this can pose unique challenges. Many of the cybersecurity risks of teleworking are not fully known or adequately communicated. And cyber threats continue to abound.

The breach at the Department of Health and Human Services underscored the continued cyber threats. In addition, news about the coronavirus is evolving by the hour. It can be daunting to separate fact from fiction and discover the latest advice you can trust about how to minimize the cyber risks to your organization about teleworking.

In this candid discussion, you'll learn from a few of the country's top cybersecurity experts about the risks we face going forward and the ways to enhance cybersecurity:

- How to implement the best practices in cybersecurity and teleworking.
- How to identify the value of your information at risk.
- How to coach and train your workers to best protect their systems and data.
- How can teleworkers protect their privileged information.
- Elasticity--how to surge and add new capacity.
- Implementing the best practices in videoconferencing and document sharing.

To register for this free webinar on Friday, April 15 at 2:00 PM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Like-farming, also known as ***like-harvesting***, is a social engineering technique that fraudsters employ to increase online engagement and boost the popularity of social media posts and pages. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Zoom Founder Promises to Remedy Security, Privacy Concerns During a "Feature Freeze"
Analytic Comment: Video teleconferencing platform, Zoom, has vastly increased in popularity and the demand for these types of tools added an additional 10 million users since December. Despite its vast user base, including schools, businesses and governments, it has its share of security issues. To address these concerns, Zoom's founder has apologized for the platform's privacy and security shortcomings and is working on corrective measures.

Microsoft Expands Security Offerings to Election Officials
Analytic Comment: Microsoft is expanding its Defending Democracy program to offer additional cybersecurity products to state and local election officials. Among these offerings is AccountGuard, previously only available to campaigns and political parties, which provides notifications about cyber threats an incidents to users of Outlook, Hotmail, and Office 365 products, will be accessible to state and local officials as well as members of Congress and their staff. Other offerings include discounted access to Microsoft's Detection and Response team and a set of recommendations for election officials to maintain voting systems and continuity in light of the current public health crisis. Microsoft suggests election officials should plan on providing voters increased access to absentee voting and allowing voters to request these ballots online.

Patches and Updates

Google Releases Security Updates
Mozilla Patches Critical Vulnerabilities in Firefox, Firefox ESR
Mozilla Releases Security Updates for Firefox, Firefox ESR

ICS-CERT Advisories

Advantech WebAccess/NMS
B&R Automation Studio
Fuji Electric V-Server Lite
GE Digital CIMPLICITY
HMS Networks eWON Flexy and Cosy
KUKA.Sim Pro
Synergy Systems & Solutions HUSKY RTU (Update A)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-04-022

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 16, 2020

National Capital Region Cyber Threat Spotlight

NASA Observes Increased Cyber Attacks

The National Aeronautics and Space Administration (NASA) has reported a significant increase in phishing attacks, malware attacks, and malicious sites targeting its personnel working from home during the COVID-19 pandemic. The agency's Security Operations Center (SOC) has been using its mitigation tools and measures to successfully block waves of cyber attacks, some of which originate from state-sponsored hackers, but warn employees to remain vigilant when opening emails. These threat actors are actively searching to trick victims into revealing sensitive personal information and account credentials, even targeting mobile devices with text messages or advertisements with applications designed to make unsuspecting victims click on malicious links. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this or any other campaign, notify your organization's IT security team immediately.***

Federal Partner Announcement

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory to provide guidance on the North Korean cyber threat for the international community, network defenders, and the public. The advisory highlights the cyber threat posed by North Korea – formally known as the Democratic People's Republic of Korea (DPRK) – and provides recommended steps to mitigate the threat. ***The NTIC Cyber Center recommends all network administrators review CISA Alert AA20-106A and implement the recommended mitigation strategies.***

Current and Emerging Cyber Threats

Hoaxcalls Botnet Targets Grandstream UCM6200 Appliances and Draytek Vigor Routers

The Hoaxcalls botnet is actively targeting a critical SQL injection vulnerability (CVE-2020-5722) residing within the Grandstream UCM600 series of IP PBX communications appliances and uses specially crafted HTTP requests to execute shell commands or inject HTML code into password recovery emails. The Hoaxcalls botnet targets compromised devices with distributed denial-of-service (DDoS) attacks. This botnet also targets Draytek Vigor routers, exploiting another critical vulnerability (CVE -2020-8515) to infect them and execute arbitrary commands. ***The NTIC Cyber Center recommends administrators of these vulnerable devices apply the latest security patches as soon as possible.***

New Dark Nexus Botnet Discovered Targeting IoT Devices

Researchers at Bitdefender discovered a new botnet dubbed Dark Nexus that targets and compromises IoT devices such as routers, video recorders, and thermal cameras and further uses them for distributed denial-of-service (DDoS) attacks and malware campaigns. Dark Nexus shares code with the Qbot and Mirai botnets, features custom-made payloads for twelve different CPU architectures, and has 40 different versions. Dark Nexus abuses various security vulnerabilities via Telnet credential stuffing and exploits on various IoT devices. ***The NTIC Cyber Center recommends users and administrators of IoT devices change default passwords and only use***

lengthy, complex, and unique credentials to secure them, monitor networks for suspicious activity, and ensure that all device firmware is patched and kept up-to-date.

Study Finds Many Android Apps Contain Backdoors

Various security researchers have discovered that a large number of Android mobile apps conduct invasive background activity. One study showed that Android apps gather information about other apps installed on the device, which could be used to document user behavior. Another study revealed that 12,706 out of 150,000 analyzed apps created possible backdoors into devices and an additional 4,028 apps verify user input against blacklisted words including the names of political leaders, news-worthy incidents, and racial discrimination. Additionally, "bloatware" apps that come preinstalled on some Android devices tend to perform a lot of this type of invasive behavior. ***The NTIC Cyber Center recommends users only download mobile applications from trusted and vetted sources and read user reviews carefully for possible indications of suspicious behavior. If the device permissions required by an app do not match the advertised functionality, refrain from installing it.***

Malwarebytes Brand Abused in Malvertising Campaign

The Malwarebytes threat intelligence team is investigating a malicious advertising (malvertising) campaign that is replicating the Malwarebytes website and infecting unsuspected victims with the Raccoon variant of information-stealing malware. This malicious advertisement is likely associated with adult websites and redirects victims to the malicious malwarebytes-free[.]com website without any user interaction. This fraudulent website is embedded with the Fallout exploit kit that enables the Raccoon infection. Malwarebytes reported that this domain was registered on March 29, 2020 and is hosted in Russia. ***The NTIC Cyber Center recommends users maintain awareness of this and similar campaigns, keep antivirus software updates with the latest virus definitions, and use a reputable ad-blocker to protect against malicious advertisements. Additionally, we recommend network administrators review the Malwarebytes report and block the associated indicators of compromise (IoCs).***

Magento Users Urged to Update to Reduce Risk of Payment Skimming Attacks

Online vendors are encouraged to update Magento, used for e-commerce transactions, to the latest version before it expires to avoid security vulnerabilities. Magento version 1.x will reach its end-of-life (EoL) status in June 2020. Magento 2.x features enhanced security, performance, and scalability. Online merchants failing to upgrade will face increased security risks including the potential for account data compromise, malicious code injection, and payment skimming attacks. ***The NTIC***

Cyber Center recommends system administrators using the Magento platform on e-commerce sites immediately upgrade it to the latest version.

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Maze Ransomware Group Targets Oil Firm

Researchers at Under the Breach, a company that monitors data breaches, stated that on April 1, 2020, oil firm Berkine was victimized in a Maze ransomware attack. The threat actors behind the attack stole an entire database containing over 500MB of confidential data and leaked information associated with the Sonatrach oil firm. The French National Agency for Security of Information Systems (ANSSI) labels the Maze ransomware group as the biggest threat to organizations worldwide, because it uses a variant of ChaCha20 cryptographic algorithm and uses extreme tactics such as blackmail to extort victims.

Travelex Pays $2.3 Million in Sodinokibi Ransomware Attack

Travelex, an international foreign exchange service provider, recently reported falling victim to a Sodinokibi ransomware attack on December 31, 2019. Sodinokibi, also known as REvil, encrypts data on computers running the Windows operating system, disables recovery mode, and deletes Volume Shadow Copies to prevent victims from trying to restore impacted files without paying the ransom. Travelex paid the threat actors behind the campaign $2.3 million to regain access to their data and continue operations. The threat actors also claimed to have stolen 5GB of personal data that supposedly includes dates of birth, Social Security numbers, and credit card data. The incident is still under investigation.

Vulnerabilities

Microsoft Exchange

Cybersecurity firm, Rapid7, revealed that 82.5 percent of Microsoft Exchange servers are vulnerable to CVE-2020-0688, a flaw that allows threat actors to compromise vulnerable Microsoft Exchange servers. This flaw is attributed to the default-enabled Exchange Control Panel (ECP) component in which threat actors can leverage previously stolen credentials to gain access. Microsoft has released a patch to fix the vulnerability. ***The NTIC Cyber Center recommends administrators of Microsoft Exchange servers apply the associated patch as soon as possible to reduce the risk of exploitation and compromise.***

Data Leaks and Breaches

Email service provider Email.it suffered a data breach in which company data and customer data associated with 600,000 users was placed on the dark web for sale. Along with Email.it's source code, the threat actors claim to have stolen customer passwords, email contents, security questions, and SMS messages sent through Email.it's SMS-sending service. The threat actors known as the No Name (NN) Hacking Group claimed to have conducted the breach more than two years ago. The breach did not affect paid accounts, but only free accounts used between 2007 to 2020. ***The NTIC Cyber Center recommends Email.it customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, or other avenues as a result of this data exposure. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication. Additionally, we also recommend Email.it users monitor associated payment accounts and report any suspicious and unauthorized activity to their financial institutions.***

Upcoming Webinars

ASMGi

SafeBreach

Can You Validate Your Security Controls in a WFH Environment?

Validating the efficacy of security controls is a challenge every organization faces. Now, with the sudden move to a full remote workforce, organizations need to safeguard their employees and company's network more than ever. Join us to learn how Breach and Attack Simulation (BAS) delivers automated continuous validation of your enterprise security controls and specifically how quickly and easily you can gain visibility and close potential security gaps while supporting a remote workforce. In this webinar we will discuss:

- How to validate and improve your security posture
- The risks your employees are exposed to when working from home
- How to validate security controls associated with remote and VPN access
- How you can test exfiltration methods to protect sensitive data leaking from employees home environment

To register for this free webinar on Thursday, April 16 at 1:00 PM EDT, click here

---

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A ***dark pattern*** is a type of social engineering technique whereby businesses or other organizations use crafty user interface/user experience (UI/UX) designs to manipulate users into making unintended choices. Dark patterns are often used to charge unwitting customers money, maintain a user's attention, harvest personal data, gain or retain subscribers, and display advertisements. While most of these tactics are not necessarily illegal, they can cost customers time, money, and privacy. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Enterprises Regard the Cloud as Critical for Innovation, but Struggle with Security
Analytic Comment: According to a recent survey, while most enterprises are willing to adopt cloud technology, only 40 percent have taken steps to manage its security. While the majority of these organizations have guidelines and policies in place, 25 percent stated that these policies were not enforced and 17 percent stated that they lacked guidelines all together. Additionally, 49 percent of the organizations included in the study claimed that developers and engineers have ignored or circumvented cloud security and compliance policies. This underscores the importance of enforcing an enterprise-wide adoption of best practices for cloud security.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Intel Releases Security Updates

Juniper Networks Releases Security Updates

Microsoft Releases April 2020 Security Updates

Oracle Releases April 2020 Security Bulletin

VMware Releases Security Updates for VMware Directory Service

VMware Releases Security Updates for vRealize Log Insight

ICS-CERT Advisories

Eaton HMiSoft VU3

Siemens Climatix

Siemens IE/PB-Link, RUGGEDCOM, SCALANCE, SIMATIC, SINEMA

Siemens KTK, SIDOOR, SIMATIC, and SINAMICS

Siemens SCALANCE & SIMATIC

Siemens SIMATIC S7 (Update B)

Siemens SIMOTICS, Desigo, APOGEE, and TALON

Siemens TIM 3V-IE and 4R-IE Family Devices

Triangle MicroWorks DNP3 Outstation Libraries

Triangle MicroWorks SCADA Data Gateway

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-04-029

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 23, 2020

National Capital Region Cyber Threat Spotlight

Over 267 Million Stolen Facebook Profile Details for Sale on Dark Web

Security researchers recently discovered that a database containing details from over 267 million Facebook profiles is currently being sold on the dark web for approximately $600. Although researchers verified that passwords were not included in the database, they did confirm that it contains Facebook users' names, phone numbers, unique Facebook IDs, and email addresses. The exposure of this information could put affected Facebook users at risk of exploitation via phishing campaigns, malicious SMS messages, and other social engineering schemes. ***The NTIC Cyber Center recommends all Facebook users remain vigilant for phishing and SMS-based social engineering campaigns, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or providing sensitive and personal information during unsolicited calls or in response to unsolicited emails.***

Federal Partner Announcement

Alert: Continued Exploitation of Pulse Secure VPN Vulnerability

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert to warn of the continued exploitation of the vulnerability present in unpatched instances of the Pulse Secure Virtual Private Network (VPN). According to CISA, unpatched Pulse Secure VPN servers continue to be an attractive target for malicious actors. Affected organizations that have not applied the software patch to fix an arbitrary file reading vulnerability, known as CVE-2019-11510, can become compromised in an attack. Although Pulse Secure disclosed the vulnerability and provided software patches for the various affected products in April 2019, CISA continues to observe wide exploitation of CVE-2019-11510. CISA expects to see continued attacks exploiting unpatched Pulse Secure VPN environments and strongly urges users and administrators to upgrade to the corresponding fixes. ***The NTIC Cyber Center recommends all network administrators review CISA Alert AA20-010A and implement the recommended mitigation strategies.***

Current and Emerging Cyber Threats

Agent Tesla Now Steals Wi-Fi Passwords

Some variants of Agent Tesla, an information-stealing malware variant with remote access capabilities, have been upgraded to steal Wi-Fi passwords. These new variants steal system information that includes data about FTP clients, browsers, file downloaders, usernames, computer names, OS names, CPU architecture, and RAM. Agent Tesla is usually distributed via malicious email campaigns and is popular among business email compromise (BEC) scammers who use it to obtain screenshots and log victims' keystrokes. ***The NTIC Cyber Center recommends users remain vigilant for malicious email campaigns disguised as official correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign or infected with Agent Tesla, notify your organization's IT security team immediately.***

Over 500,000 Zoom Account Credentials Found for Free on Dark Web and Hacker Forums

Cybersecurity intelligence firm Cyble recently discovered that more than 500,00 Zoom account credentials were being offered on various dark web and hacker forums for free. BleepingComputer researchers have been contacting compromised email addresses and have verified that the stolen credentials are currently valid. Cyble has since purchased approximately 530,000 Zoom credentials to warn customers of the breach and reset victims' passwords. ***The NTIC Cyber Center recommends that all Zoom users change their account credentials immediately, using lengthy, complex, and unique passwords, and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise.***

New MBR-Wiping Malware Impersonates Security Researchers

Unidentified cyber threat actors have been locking victims' computers with a Master Boot Record (MBR) wiper or MBR locker while trying to frame cybersecurity researchers as perpetrators. When victims download and install free software from unvetted sources, their systems can become infected with the MBR wiper malware, which prevents the operating system from booting properly. The screen then displays a message that includes contact information for the hackers and instructions on how to obtain an "unlock code" to restore their systems. ***The NTIC Cyber Center recommends users only download applications from trusted and vetted sources, keep device operating systems up to date, and maintain regular backups of critical files and software to protect against the threat of MBR wipers.***

WooCommerce Targeted in Magecart Card Skimming Attack

WordPress e-commerce sites that have the WooCommerce plugin installed are being targeted by credit card thieves who exploit a vulnerability using JavaScript-based card-skimming malware. This malware modifies payment details within the WooCommerce plugin and forwards customer payments to financial accounts controlled by the attackers. Known as Magecart attacks, e-commerce sites have commonly become targets for profit-motivated cyber threat actors seeking to steal payment card data from unsuspecting victims. ***The NTIC Cyber Center recommends administrators of Wordpress-powered e-commerce sites disable direct file editing for wp-admin. Bleeping Computer provides instructions here.***

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

"Double Extortion" Ransomware Campaigns Increase

Double extortion, the tactic of publishing data stolen from victims who do not remit payment from ransomware, has gained popularity among profit-motivated cyber threat actors. The stolen information is often used to motivate victims to pay the ransom to prevent sensitive information from being publicly revealed since, over the years, organizations have avoided paying by restoring data from backups. The threat actors behind the Maze ransomware variant first started this current trend in late 2019, and then those behind the Clop, Sodinokibi/REvil, Nemty, and DoppelPaymer ransomware campaigns quickly adopted the same tactics. However, paying the ransom in a double extortion scheme does not guarantee that the threat actors will not publicly release the stolen data in the future.

Maze Ransomware Targets Managed Service Provider

On Friday April 17, 2020, information technology firm Cognizant discovered that Maze ransomware operators had breached their network for weeks, if not longer. Recent research suggests that ransomware operators may explore a targeted network for a period of time before deploying the malware and encrypting data. Because Cognizant is an IT managed service provider, the company notified all clients that they had been compromised as well. This incident highlights the risk that compromised managed service providers can pose to networks and systems.

Data Leaks and Breaches

The US Small Business Administration (SBA) announced on April 22, 2020 that business owners who applied for an Economic Injury Disaster Loan may have had their personal information

exposed. A flaw within the SBA application portal allowed some loan applicants to view the personal identifiable information (PII) of other applicants. The PII exposed includes names, Social Security numbers, tax ID numbers, addresses, dates of birth, email addresses, phone numbers, marital and citizen status, income, and other information. No external exposure to the data was reported. Although there has been no evidence of anyone abusing this information, the SBA is offering all affected business owners free identity theft protection services for one year. ***The NTIC Cyber Center recommends affected business owners register for the free identity theft monitoring services offered, remain vigilant for phishing, vishing, and SMSishing campaigns associated with this breach or loan application, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources.***

Researchers at vpnMentor discovered a breach of energy workforce company RigUp resulting in the exposure of more than 70,000 private files. The exposed data includes names, addresses, dates of birth, Social Security numbers, phone numbers, addresses, resumes, private photos, professional IDs, professional certificates, and insurance plan information. The breach is attributed to improperly secured Amazon Web Services (AWS) S3 buckets. RigUp stated that they would conduct a root cause investigation after being notified. It is unknown if any threat actors abused the exposed data. ***The NTIC Cyber Center recommends RigUp clients remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. We also recommend RigUp clients monitor associated vendor accounts and report any suspicious and unauthorized activity to their financial institutions.***

Upcoming Webinars

The New Normal & How This Is Impacting Cybersecurity When Building Your business Continuity Plan

With recent events, everyone is talking about remote access and working remotely. Some businesses are looking at this as potentially the new norm that is changing how we are connecting with the

business world and each other. Business are looking to have security embedded in their strategy and solutions, in order to minimize their exposure to risk as much as possible.

In this webinar, Fortinet will be reviewing some of these new business challenges, as well as some strategies for every cybersecurity leader to consider when building a secure remote connectivity solution that can scale.

To register for this free webinar on Tuesday, April 28 at 9:00 PM EDT, click here

---

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for financial gain or identity theft. Perpetrators take advantage of the numerous steps taken and parties involved in the real estate acquisition process. They target victims using email, voice messaging services, and websites. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Linksys Prompts Password Reset to Prevent Router Hacking
Analytic Comment: Linksys Smart Wi-Fi users are urged to change their passwords due to a surge of fraudulent COVID-19 messages appearing on user's browsers prompting them to download malware. In this attack, threat actors leverage stolen credentials from other websites to access the victim's router and alter its settings to display malicious websites. Additionally, users are also encouraged to verify the accuracy of the router's DNS settings and making sure their antivirus