FEMA Region III Cyber Security Program

Maryland Cyber Security Workshop (January 16, 2019)

(Presented again at the October 16, 2018, meeting of the Maryland Cybersecurity Council and published with permission.)

FEMA

Overview

- Current Landscape
- Challenges
- Review current resources (Federal and State)
- Discuss information flow for reporting an incident
- Discuss what prompts a report and determines who is called
- FEMA's Role in a Cyber Incident and Region III's workshops

FEMA

Current Landscape

- Cybersecurity is not “solvable”
  - State and Territory Self-Reported Capability Levels - Cybersecurity is the lowest rated of the capabilities
- Progress has been made, but more needs to be done
  - Cybersecurity roles and responsibilities across the stakeholder community remain unclear
    - Feedback from State Partners – *who do we call for an incident? Which federal partner is the lead? How do we get better information? – need DHS and FEMA HQ to continue these discussions*
  - All-hazard doctrine has started to, but does not fully address the impacts of cybver events
  - Training and exercises will be required to continue to institutionalize cyber preparedness and response
  - Cross stakeholder coordination is essential and must grow past the “get to know each other” phase

FEMA

Challenges Surrounding Responding to Cyber Incidents

- End User Error
- No geographic boundary
- Fast spreading
- Often must do investigation, mitigation and response all at one time

FEMA

Federal Resources – Asset Response

- DHS National Cybersecurity and Communications Integration Center (NCCIC)
  - Is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications for the federal government, intelligence community and law enforcement
  - Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Federal Resources – Asset Response

- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Responds to and analyzing control systems-related incidents;
  - Conducts vulnerability, malware, and digital media analysis;
  - Provides onsite incident response services;
  - Provides situational awareness in the form of actionable intelligence;
  - Coordinates the responsible disclosure of vulnerabilities and associated mitigations; and
  - Shares/Coordinates vulnerability information and threat analysis through information products and alerts.

Federal Resources – Asset Response

- DHS United States Computer Emergency Readiness Team (US-CERT)
  - Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
  - Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
  - Responding to incidents and analyzing data about emerging cyber threats.
  - Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

Federal Resources – Asset Response

- USCG National Response Center (NRC)
  - Maritime centric
  - The NRC usually deals with chemical/oil/hazmat spills, if they get a cyber report it is shared with the DHS NCCIC
  - Maritime entities can all the DHS NCCIC directly but must report that they are a Coast Guard regulated entity in order to satisfy the reporting requirements of 33 CFR part 101.305

Federal Resources – Threat Response

- FBI Field Office Cyber Task Forces
  - Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

- FBI Internet Crime Complaint Center (IC3)
  - Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

- FBI National Cyber Investigative Joint Task Force
  - Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government

Federal Resources – Threat Response

- United States Secret Service Field Offices and Electronic Crimes Task Forces
  - Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

- United States Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI)
  - Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

Federal Resources – Intelligence Support

- Office of the Director of National Intelligence (ODNI) through Cyber Threat Intelligence Integration Center (CTIIC)
  - Provides integrated all-source analysis of intelligence related to foreign cyber threats or incidents affecting U.S. national interests;
  - Supports federal cyber centers by providing access to intelligence necessary to carry out their respective missions;
  - Oversees development and implementation of intelligence sharing capabilities to enhance shared situational awareness;
  - Ensures that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both U.S. Government and U.S. private sector entities;
  - Facilitates and supports interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

Intelligence/Information Resources

- FBI Infraguard
  - InfraGuard is a partnership between the FBI and members of the private sector. Infraguard is dedicated to information sharing and relationship building across organizations including state and local law enforcement agencies. While it also has a physical security focus, the program started with a cybersecurity case in 1996. Its 85 chapters hold meetings and training sessions around topics that benefit members and develop special interest groups to address topics like cybersecurity in-depth.

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - As part of the Center for Internet Security, the MS-ISAC offers free managed security and advanced monitoring services to state, local, tribal and territorial governments. As of 2011, the center was working with all 50 states and was home to a first-of-its-kind facility that's staffed 24/7 to guard against electronic attacks on government systems and information.

Intelligence/Information Resources

- National Governors Association
  - The association's Resource Center for State Cybersecurity aims to provide governors with resources and tools for implementing effective policies and practices on the topic. Launched in 2012, the initiative's primary goal is for states to develop strategies for strengthening cybersecurity practices as the relate to IT networks, health care, education, public safety, energy transportation, critical infrastructure, economic development and the workforce.

- NIST Framework for Improving Critical Infrastructure Cybersecurity
  - The framework is a living document of best practices that uses can reference to establish a risk-based approach to improve cybersecurity. The latest draft was released in January 2017. It provides a series of actions to anticipate and respond to attacks on systems.

Intelligence/Information Resources

- National Guard Cyber Protection Teams
  - Cyber Command Readiness Inspections
  - Vulnerability Assessments
  - Cyber opposing force support (threat emulation)
  - Critical Infrastructure Assessment

- DHS Cyber Security Advisors (CSA)
  - Great resource for information/trends
  - Region III CSA: Franco Cappa

FEMA

Intelligence/Information Resources

- FEMA Region III Cyber Incident External Affairs Resource Guide
  - The purpose of this document is to describe the role of FEMA External Affairs in the event of a cyber incident and have resources readily available to support unified messaging priorities.
  - The intended audience for this document is FEMA Region III External Affairs staff. Other Region III staff members may also benefit from understanding the role of External Affairs in the event of a cyber incident.
  - The role of FEMA External Affairs in regards to cyber incidents is essentially threefold:
    1. Promote cyber security to individuals and organizations.
    2. Support information sharing with our federal, state, and local partners in the event of a significant cyber incident.
    3. Participate in cyber security exercises, such as the 2012 National Level Exercise.

FEMA

State Resources - Reporting

- DC Washington Regional Threat Analysis Center
- Delaware Information and Analysis Center
- Maryland Joint Operations Center
- Pennsylvania State Police Criminal Intelligence Center
- Virginia Fusion Center
- West Virginia Intelligence Fusion Center

FEMA

Triggers to report a Cyber Incident

- What triggers would occur to make you contact someone (state or federal for assistance)?
  - Potential Guide from National Cyber Incident Response Plan:
  - **Level 0: Nuisance DoS or defacement** *(No event or incident anticipated. This includes routine watch and warning activities.)*
  - **Level 1: Commit a financial crime** *(Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)*
  - **Level 2: Steal sensitive information** *(May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)*
  - **Level 3: Corrupt or destroy data/Deny availability to a key system or service** *(Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)*
  - **Level 4: Damage computer and networking hardware** *(Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.)*
  - **Level 5: Cause physical consequence** *(Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.)*

FEMA's Role in Cyber Incidents

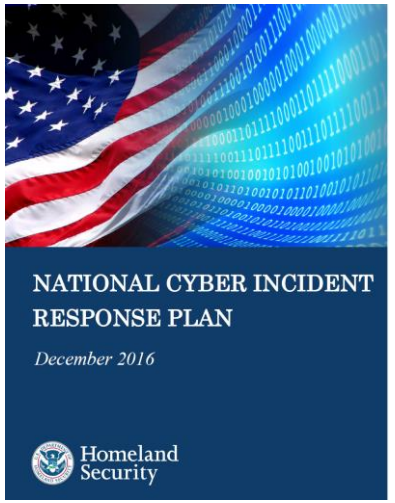
- FEMA's role in the federal government's response to and recovery from a cyber incident is outlined in the National Cyber Incident Response Plan (NCIRP), which was developed by DHS's National Protection and Programs Directorate (NPPD) and FEMA's National Integration Center in coordination with interagency partners

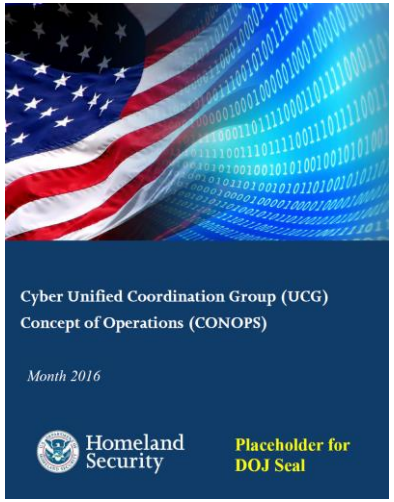
- Existing policies and coordinating structures can handle the vast majority of cyber incidents, however significant cyber incidents may require the establishment of a Cyber Unified Coordination Group (UCG)

- Depending on the response activities needed to support the incident, FEMA may activate certain ESFs. The significant cyber incident response mechanisms outlined in the NCIRP's Coordinating Structures and Integration section will coordinate with the established ESFs

National Cyber Incident Response Plan (NCIRP)

- NCIRP sets forth:
  - Roles and responsibilities of federal, state, local, territorial and tribal (SLTT) partners, private sector, and international stakeholders
  - Incident Severity Schema
  - Coordination structure and required capabilities to respond
- A Cyber Unified Coordination Group (UCG) will function as the primary method for coordinating between and among federal agencies.
- Download the NCIRP at www.us-cert.gov/ncirp





	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

FEMA

NCIRP and FEMA

- FEMA's emergency management responsibilities:
  - FEMA is the Lead Federal Agency for coordinating the response to physical impacts of a cyber incident.
  - Anticipate supplemental non-Stafford Act support requests from DHS National Protection and Programs Directorate (NPPD) and FBI (operational coordination, situational awareness, crisis action planning), if needed.
  - Maintain the continuity of disaster functions when systems are down or vulnerable (either analog or manually).

- FEMA (NCP) provides direction to federal departments and agencies through continuity directives and guidance to non-Federal Governments through Continuity Guidance Circulars on Continuity Planning for Cyber threat.

FEMA

Effects on COOP following a Cyber Incident

- If the Nation faces a significant cyber incident today:
  - Offline systems leave an elevated national security risk and keep government services from reaching survivors
  - A significant cyber incident could take out many mission essential and/or vulnerable legacy federal IT systems
  - SLTT governments do not have IT mechanisms in place to engage in continuity of operation activities

- Continuity Directives 1 and 2 (2017)

- Resilient Accord Workshop—Continuity for Cyber Threat:
  Conducted throughout the Nation
  To improve whole community COOP planning for a cyber threat

FEMA

FEMA Region III Cyber Security Workshops

- Region III has hosted 3 workshops to date:
  - August 17-18, 2016 Workshop and TTX in Philadelphia, PA
    - Panels from federal, state and private sector partners
    - Presentation on National Cyber Incident Response Plan
    - Tabletop Exercise on Cyber Incident
  - July 25, 2017 Workshop in Suffolk, VA
    - Panel from state partners
    - Presentations on VA National Guard Cyber Teams, VA Fusion Center, FEMA Region III Cyber 411 Resource Guide, National Cyber Incident Response Plan
  - July 18, 2018 Workshop in Annapolis, MD
    - Panels from federal and state partners
    - Presentations on TEEX resources and Cyber Attack Demo, RAND study on Cyber Plans
  - Looking to partner with Delaware to host our next workshop in the summer of 2019

FEMA

FEMA