

**WASHINGTON
CYBERSECURITY
SITUATIONAL
AWARENESS CONCEPT
OF OPERATIONS
(CONOPS)**

Table of contents	
INTRODUCTION	3
1.1 Purpose	3
1.2 Background	3
1.3 Scope	3
1.4 Objectives	4
Current options and processes for reporting	4
2.1 Justification for a single point of contact reporting at the state and local level	4
2.2 US Coast Guard	4
2.3 Department of Homeland Security and Federal Law Enforcement	5
2.4 Local Law Enforcement and Intelligence – Washington State Fusion Center	5
Local and Statewide Reporting Operations	6
3.1 OVERVIEW	6
3.2 CATEGORIES	6
3.3 INCIDENT REPORTING TO WASHINGTON STATE FUSION CENTER (WSFC)	7
Submission, Analysis, and Dissemination	8
4.1 Analysis of Agency Incident/Event Data	8
4.2 Severity Rating	9
4.3 WSFC Products related to Cyber incident response	10
4.3.1 WSFC After Action Reports	10
4.3.2 Fusion Center Insider monthly publication	11
4.4 On-site Incident Response Assistance for Agencies	11
4.5 Incident Escalation	11
4.6 Notification of other related organizations, emergency management, and law enforcement	11
4.7 Communications	12
4.7.1 Communication During an Incident	12
4.7.2 Communication Guidelines	12
4.8 Regulatory Requirements	13
5.0 Securing and safeguarding information	13
5.1 Confidentiality	13
Definitions	13
5.2 Outreach and education	14
Appendix A - Contact information	15
Appendix B - Regulatory requirements	17
Appendix C - DOJ CTF compromised Computer network incident worksheet	19

Appendix D - Acronyms	24
Appendix E - SLTGCC Cybersecurity Resource Compendium	26
Appendix F - Washington State Partner Cyber Response Template	27

1 INTRODUCTION

1.1 Purpose

The purpose of the Cyber Resilience CONOPS is to enable the sharing of information and analysis that can assist state, local and tribal agencies, and public and private sector critical infrastructure providers and key resource stakeholder organizations in the performance of their public safety, security, continuity, and disaster resilience responsibilities. This CONOPS focuses on Cyber Security Incident reporting and response in Washington State. It suggests processes, protocols, and policies that any stakeholder organization can put into practice to increase their resilience and response capabilities before, during and after a serious cybersecurity incident. It includes suggestions for tools and specific guidelines by which an organization will be able to better detect, triage, and respond effectively to a cybersecurity intrusion or compromise. It specifically includes guidance for engaging with the local cyber community, including public and private sector partners, law enforcement, and State and Federal resources.

1.2 Background

The Pacific Northwest Economic Region (PNWER) and its Center for Regional Disaster Resilience (CRDR) have been awarded a 2017 National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge grant for the Cyber Resilience Category. Prior to this award, PNWER led several exercises and workshops focused on cybersecurity information sharing capabilities across the region. Stakeholders consistently identified a gap in cyber reporting capabilities and recommended a process to ensure local and state emergency management and law enforcement receive cyber-related incident reports. The current DHS recommended practice is to send cyber threat and vulnerability reports to the DHS National Cybersecurity and Communications Integration Center (NCCIC). This process creates a significant delay in real-time situational awareness for state and local government and industry-wide stakeholders. After meeting with stakeholders and conducting a survey to assess the current state of cyber resilience amongst Maritime and other entities in the region, we have expanded the scope to include more of the interdependent organizations at the recommendation of the stakeholder advisory group. We are currently working with the Washington State Fusion Center as a focus of communications for organizations to report incidents and to be directed to appropriate resources. WSFC will directly communicate to the reporting agency as well as all affected agencies to provide a status update and suggested mitigation or response activities. Currently, the WA Fusion Center is not a 24-7 center. This effort falls in line with 2013 and 2016 presidential directives on information sharing:

- <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

1.3 Scope

This CONOPS is designed to address the needs of all organizations, public, private, academic, and non-profit in the Puget Sound region with a primary focus on critical infrastructure and key resources (CI/KR). As this includes critical infrastructure, it will include specific references to regulatory and best practice guidance toward response notification and resource and information sharing within the cyber community of the Puget Sound area and its dependent neighbors.

1.4 Objectives

- **Create a working concept of operations to which organizations can and will turn to for guidance on when, how, and whom to notify during a significant cyber incident.**
- **Provide a single point of contact for reporting significant cyber incidents**
- **Provide information and analysis, advisories, and two-way cross-sector information support to cyber preparation, planning, and response and recovery efforts.** The Critical Infrastructure Key Resources (CI/KR) component of the Washington State Fusion Center supports the objective to serve as an information sharing and analysis mechanism to assist state, regional, and local emergency operations centers, first responders, and critical infrastructure sectors during disasters. The fusion center does this by providing situational awareness during disasters or significant criminal or terrorist events. This includes processing information to provide threat assessments that assist agencies and critical infrastructure providers and other essential service providers with their planning and preparation efforts related to cybersecurity.
- **Encourage notification and information sharing across sectors and jurisdictions**

2 CURRENT OPTIONS AND PROCESSES FOR REPORTING

2.1 Justification for a single point of contact reporting at the state and local level

Currently, several federal agencies collect significant cyber incident reports through different portals or websites. Often these reports do not get shared in a timely manner with state, local and regional partners. This lag in information sharing is a significant threat to the overall resilience of the region. Often agencies have a regulatory requirement to report to federal partners and must follow strict protocols. We encourage federal partners to work with regional, state and local partners to ensure information is disseminated and shared at all levels. Organizations who do have a regulatory requirement to report to a federal agency are encouraged to utilize the WA State Fusion Center (WSFC) reporting portals, email or phone number to report cyber threats and disruptions. The WSFC will work with state, local and regional CI/KR stakeholders to share information to improve preparedness and resilience across all sectors. Likewise, the fusion center along with the DHS Cybersecurity Advisor (CSA) will serve as valuable advisors on potential resources or assistance available to organizations.

The following are the most likely partners collecting reports on significant cyber events base on stakeholder survey input.

2.2 US Coast Guard

The Coast Guard is the principal Federal agency responsible for the maritime safety and security of U. S. ports and waterways and has legal authorities within the maritime transportation system (MTS).[i] Maritime infrastructure includes vessels, facilities, ports, bridges and other systems that operate within the maritime domain. Vessels and facilities regulated by the Maritime Transportation Security Act (MTSA) report cyber incidents to the National Response Center (NRC), or, for cyber incidents that do not involve physical or pollution effects, the NCCIC.[ii] The NRC notifies the appropriate Coast Guard Captain of the Port. Within the state of Washington, responding Coast Guard units report MTS cyber incidents to the Washington State Fusion Center and appropriate Area Maritime Security Members.[iii]

[i] 14 U.S.C § 89, 33 U.S.C § 1223, 14 U.S.C. § 91, 50 U.S.C. 191

[ii] 33 CFR part 101.305

[iii] Cyber Incident Response Guidelines for Maritime Transportation Security Act (MTSA) Regulated Facilities and Vessels, PACAREAINST 16600.1

2.3 Department of Homeland Security and Federal Law Enforcement

The DHS NCCIC has a wide variety of resources available to assist organizations with their cyber risk assessments, penetration testing, as well as procedure and policy development, following the NIST 800-53 guidance. DHS encourages organizations to report incidents, especially if they affect critical infrastructure or security. Similarly, the FBI has online tools for reporting cyber incidents and encourages anyone to report using those tools. The local offices of the US Secret Service participate in an Electronic Crimes Task Force which specifically will work with organizations that have suffered a financial loss or crime. Contact information for these organizations is included in Appendix A.

However, it should be noted that while these are important and valuable resources for reporting and possibly for a response, they bypass local law enforcement and emergency management organizations and thus may result in a lack of capability to respond to events that affect others in the local community.

2.4 Local Law Enforcement and Intelligence – Washington State Fusion Center

The Washington State Fusion Center (WSFC) is a clearinghouse for local, State, Federal, Tribal and Territorial law enforcement information and Intelligence gathering organizations. To meet the objective of this CONOPS we intend to establish a central contact within the WSFC which would serve the cyber community as a connection to the appropriate resources during a significant cyber incident. WSFC collects, writes, and disseminates raw reporting, produces cyber analysis based upon raw reporting and other local and national sources and analysts have sufficient cyber knowledge to receive, relay, and analyze cyber incidents and reporting. Ideally, they will be able to provide input information about the incident, and referral to the appropriate or required organizational and assistance resources. These might include the Coast Guard command center as noted above, law enforcement, DHS NCCIC, Washington State Emergency Management, The Cyber Incident Response Coalition & Analysis Sharing (CIRCAS), The National Cyber-Forensics & Training Alliance (NCFTA) or other community resources.

3 LOCAL AND STATEWIDE REPORTING OPERATIONS

3.1 OVERVIEW

It is the responsibility of any organization to combine the highest qualified and trained cybersecurity professionals, processes and technology to produce a sufficient level of technological expertise to accurately and efficiently analyze new or evolving security events. The success or failure of cyber response operations depends significantly on how accurate an organization’s security analysts judge the severity as security events emerge.

3.2 CATEGORIES

A computer incident may be defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. To clearly communicate incidents and events (any observable occurrence in a network or system) it is necessary for an organizational incident response teams to adopt a common set of terms and relationships between those terms. The following table outlines categories of incidents or events as suggested by NIST in its Special Publication 800-61.

Table 3-1 Incident Categories
***Defined by NIST Special Publication 800-61**

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency’s internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resources	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	<i>Successful</i> installation of malicious software (i.e. virus, worm, Trojan horse, or other code-based malicious entity that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection <i>if</i> widespread across the agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies	Weekly

Table 3-2 Federal Agency Event Categories

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 5	Scans/Probes/Attempted Access	This category includes an activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If the system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

3.3 INCIDENT REPORTING TO WASHINGTON STATE FUSION CENTER (WSFC)

Reports shall be transmitted in a manner consistent with their sensitivity, severity, and needed resources. Reports can be received through multiple methods depending on stakeholder preference. Reports can be submitted to the WSFC via one of the following methods:

EMAIL	intake@wsfc.wa.gov
TELEPHONE	206.262.2285
HOTLINE	1.877.843.9522
FAX	206.224.5454
Fusion Center SAR	http://www.wsfc.wa.gov/Report
NWWARN	http://nwwarn.org/alertSignup-Fusion.aspx

Reports shall include a description of the incident or event with as much of the information listed below as possible; however, reporting should not be delayed to gain additional information:

- ✓ Agency name
- ✓ Any required regulatory reporting protocols
- ✓ Point of Contact Information (name, telephone, email)
- ✓ Incident Category Type
- ✓ Incident date/time (Timezone)
- ✓ Source IP, Port, Protocol
- ✓ Destination IP, Port, Protocol
- ✓ Operating System and version, patch, etc.
- ✓ System Function (DNS/Web server, workstation, etc)
- ✓ Antivirus software installed, version, the latest update

- ✓ Location of the system(s) involved in the incident
- ✓ How was the incident identified (IDS, audit log analysis, system administrator)
- ✓ Impact to agency
- ✓ Resources or further information requested
- ✓ Resolution

Using the above information all reports to the WSFC will be submitted utilizing the reporting Network Incident Worksheet included in Addendum A – DOJ Cyber Task Force (CTF) Compromised Computer Network Incident Worksheet. All incident response teams will utilize this form when reporting incidents to the WSFC. Depending on the criticality it is not always feasible to gather all the information prior to reporting but to continue to report information as it is collected.

NOTE: Preparing this form ahead of time is a good practice that can expedite the gathering of information during an incident.

4 SUBMISSION, ANALYSIS, AND DISSEMINATION

4.1 Analysis of Agency Incident/Event Data

Once information is received as discussed above it is analyzed in-house based on WSFC best practices, technical tools, defined processes and procedures and considered for dissemination to the appropriate organizations or regulatory agencies. All reports of incidents and events received are triaged and reviewed upon receipt. Upon confirmation of incidents or events having a high severity rating, the WSFC will directly communicate to the reporting agency as well as all affected agencies to provide a status update and suggested mitigation or response activities.

4.2 Severity Rating

It is important to use a standardized, repeatable and reliable method to assess the criticality or severity of a new or emerging cybersecurity event. The initial step after gathering information is to assess its “severity” using a scale from 1 to 5, with 1 being minimal and 5 being a crisis. Factors that are weighed in determining the ‘severity’ of a security event are based upon the following matrix:

Table 4-1 Severity Table

Vulnerability	Exploit	Emerging Threat
Is the vulnerability widely known?	Method & speed of propagation	Is the threat unique?
Is exploitation of the vulnerability being reported to incident response?	Protocol & ports	Does current anti-virus signatures detect the threat (are anti-virus vendors developing new signatures to protect against the threat?)
Is the Internet infrastructure at risk?	Payload; how destructive is it?	Is this repetitive of prior attacks?
What is the number of Internet systems at risk?	How many units are known to be affected?	Likely impact on a significant part of the Internet community
What is the impact on users of exploiting the vulnerability?	Relatively speaking, how important are the systems affected?	Visibility in the press
How easy is it to exploit the vulnerability?	How many unique sites or reporters have informed us of this activity?	See also the factors for Exploit.
What is the previous access required to exploit?	What is the localized impact of this activity during the incident?	
Visibility in the press	What is the residual impact of this activity after the incident?	
	How complicated is the attack method	
	Visibility in the press	

This assessment methodology is progressive. When relevant information is received concerning a unique security event or incident, its severity rating is assigned or reassessed with the receipt of updated or new information as the event progresses. The nature of the information and its severity rating dictates the actions taken by your organization and the dissemination and communications of the WSFC.

Table 4-2 Severity Rating

Severity	Rating	Description
Minimal	1	Negligible impact on the organization.
Low	2	Very low impact on the organization. Unlikely to affect other organizations.
Medium	3	Poses a potential impact on the organization. A minimal possibility of impact to other organizations.
High	4	Has impacted the organization. Likely impact on other organizations.
Crisis	5	Has had a severe impact on the operational capacity of the organization. Known or expected impact on other organizations.

4.3 WSFC Products related to Cyber incident response

At the heart of WSFC’s mission is the need to share, on a real-time basis, relevant cybersecurity information with the organizations. Following this CONOPS the final state of the incident management process is the dissemination of information.

Currently, the WA Fusion Center utilizes the Northwest Warning Alert and Response Network and Homeland Security Information Network (HSIN) to communicate with vetted critical infrastructure stakeholders from across the state. NWWARN was formed in partnership with the Pacific Northwest Economic Region as a way to connect public and private sector stakeholders from all critical infrastructure sectors. The fusion center currently vets new members of NWWARN and organizes stakeholders by sector. Vetted stakeholders can also send messages through the NWWARN system to share information. Currently, there are over 3500 vetted stakeholders from all sectors across Washington and the surrounding region in the NWWARN database. The fusion center will utilize NWWARN as a primary way to communicate with specific sectors and jurisdictions regarding threats and warnings related to cyber incidents as well as HSIN for sensitive information sharing.

4.3.1 WSFC After Action Reports

After a severity level four or higher cyber event, WSFC would work with the Washington Emergency Management Division to pull together those involved in the incident within for an initial meeting to walk through the timeline of events and actions taken so that a more detailed after-action meeting can be held within thirty days of the cyber event. The purpose of this meeting is to conduct a detailed review of how the incident could have been prevented, a review of the response & recovery, and what the impact was. The WSFC could participate to provide feedback on what information and/or intelligence received was beneficial to understand the complexity, intent, motivations, and potential actors behind the attack. The Washington EMD would work to develop a final after action report from this working group and present to all agencies involved so that actions might be taken to prevent or decrease the amount of time it takes to recover from another incident. A copy of the report will be sent to organizational leadership, and any required regulatory agencies.

4.3.2 Fusion Center Insider monthly publication

Monthly the WSFC creates a report of the incidents that have been reported, their severity, time to resolve, and categories. This often includes a trend graph that will show incident trends over time based on category/severity.

4.4 On-site Incident Response Assistance for Agencies

As needed and appropriate based on the severity of the incident and WSFC assessment and triage, WSFC may request resources and specific cyber response assistance from either the Washington State Emergency Management or a WA State authorized cyber reserve corps entity that is responsible for the training, credentialing, risk and deployment of qualified cyber responders.

4.5 Incident Escalation

Escalation criteria are based on actual operational incident reports received and analysis performed by the WSFC. These criteria will best indicate an incident which has operational significance throughout the local cyber community. WSFC has responsibility for maintaining and updating the list below and for publishing updates to reporting agencies as necessary. Factors are weighed and verified in determining the severity of an incident based upon the following criteria:

Table 4-3 Escalation Criteria

Escalation Criteria
Any intrusion into a classified network.
Any unauthorized privileged user, administrator, or root level access of a system which crosses organization or agency boundaries.
Any incident involving a second level domain name server.
Any incident which impacts an organization's operations.
Any incident from a country against which the US is currently conducting operations or will imminently conduct operations.
Any targeted intrusion of the critical infrastructure or government networks.
Any incident involving a second level domain web server
Any new virus/worm for which no published countermeasure exists, any new virus/worm whose propagation could likely circumvent organization's containment capabilities, or any new virus/worm which affects vital network services (e.g., e-mail and DNS services).
Any root level access on a system using new methods, which exploit significant vulnerabilities shared across organization or third party systems.

4.6 Notification of other related organizations, emergency management, and law enforcement

WSFC will continue to work directly with the organizational and community incident response teams that include CIRCAS, law enforcement, intelligence community, and other related public and private sector organizations to assess the situation and continually update all parties as appropriate.

Some of these organizations will need to know an incident occurred and what its potential operational impact is at the local, state, or national level if any. While other organizations will require more technical detail, to help them better protect their information assets for which they are responsible.

4.7 Communications

Depending upon the severity and the likelihood of other organizations being affected, the WSFC will make decisions on whom and how often to communicate notice, updates, and basic information.

4.7.1 Communication During an Incident

To ensure constant communication during an incident, WSFC will maintain an open communications teleconference line immediately upon acquiring a mission number from WA State EMD and dispatching cyber responders. A 24-hour cycle will continue through the extent of an incident during the first 2 weeks. For long-term incidents, a process will be arranged between WSFC and the affected agency to ensure that ongoing communication between agency and WSFC is maintained as necessary.

Once an incident has been resolved, it essential that agencies notify and update the WSFC so that the ticket can be closed. This notification should be made through email or phone within 24 hours of resolution. Once an incident is closed out, WSFC will update the tracking system and archive the incident for future reference as needed.

4.7.2 Communication Guidelines

The matrix below provides general guidance but at the discretion of the WSFC analyst, it should be considered flexible and dynamically adjustable as appropriate to the specific incident.

Table 4-4 Communication Guidance

Severity Rating	Notifications To
Minimal (1)	Internal to organization and WSFC or other analyst personnel
Low (2)	All the above and outside analysts, Local and State agencies (WA EMD, CISO, Attorney General)
Medium (3)	All the above and Regulatory (NERC/FERC, USCG, SEC) and Federal Agencies (DHS NCCIC, FBI, USSS, ATF, US Attorney) If an organization is regulated, they must directly notify the regulatory body
High (4)	All the above and other similar organizations
Crisis (5)	All the above and CIRCAS, ISACs, ISAOs, other information sharing organizations.

4.8 Regulatory Requirements

Organizations may have specific regulatory reporting requirements. It is outside the scope of this CONOPS to detail all of those, however, each organization must be cognizant of and compliant with any required regulatory notice protocols. Many of these are referenced in Appendix B.


5.0 SECURING AND SAFEGUARDING INFORMATION



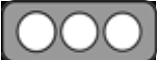
Participating organizations may expect or require that their identifying information and any specific intellectual property or other sensitive security information be protected as part of this process.

5.1 Confidentiality

Systems of collection and retention of cyber incident information will be designed to ensure confidentiality of attribution and will have mechanisms with which participating organizations can select which data is shared and with whom. Stakeholders are encouraged to use the Traffic Light Protocol as defined by US-CERT. <https://www.us-cert.gov/tlp> The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>

<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

5.2 Outreach and education

PNWER will partner with WSFC, WA Military Department, Fusion Liaison Officers, county and city emergency management, IT, law enforcement and critical infrastructure partners from across the region to provide an update on training opportunities and to promote the conops.

The WSFC will include the CONOPS procedures in its training programs including the new Cyber Liaison training program across the state.

APPENDIX A - CONTACT INFORMATION

1. WSFC/Law Enforcement - Toll Free Phone: 1-877-843-9522; Email: intake@wsfc.wa.gov
2. National Response Center (NRC) – 1-800-424-8802
3. DHS/NCCIC - To report an incident: <https://www.us-cert.gov/forms/report>. to report threat indicators: <https://www.us-cert.gov/forms/share-indicators> - 1-888-282-0870
4. Federal law enforcement (DOJ/FBI, Secret Service, ATF, US Attorney)

- United States Secret Service/Secret Service Field Offices:
(http://www.secretservice.gov/field_offices.shtml)
- Electronic Crimes Task Forces (ECTFs): <http://www.secretservice.gov/ectf.shtml>
- U.S. Department of Justice (DOJ) - Federal Bureau of Investigation (FBI)
FBI Field Offices: <http://www.fbi.gov/contact-us/field>
Cyber Task Forces: <http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1>
- Law Enforcement Online Portal: <https://www.cjis.gov/CJISEAI/EAIController> or (888) 334-4536
- CJIS: CJIS Compliance Solutions - Criminal Justice Information System
<https://safenet.gemalto.com/data-protection/data-compliance/cjis-compliance/>

5. NWWARN nwwarn.org

6. State of WA

- Office of Emergency Management - 800-258-5990,
- CISO - cybersecurity@ocs.wa.gov; 360-407-8700, 1-888-241-7597

7. Other Local Key Contact numbers:

Seattle PD: (206) 625-5011

WSP: (360) 596-4000

FBI: (206) 622-0460

DHS: (202) 282-8000

Seattle Fire: (206) 386-1400

TSA: 1 (800) 289-9673

APPENDIX B - REGULATORY REQUIREMENTS

1. North American Electric Reliability Corporation (NERC)/Federal Energy Regulatory Commission (FERC)

There are 14 mandatory NERC standards. Critical Infrastructure Protection (CIP) establishes requirements for securing the bulk power system with 11 reliability standards subject to enforcement.

<https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>

2. United State Coast Guard (USCG) Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities <https://www.regulations.gov/document?D=USCG-2016-1084-0002>

Entities that are regulated under the Maritime Transportation Security Act (MTSA) are also subject to the NVIC. Entities must be able to demonstrate how they are addressing cybersecurity risks. The NVIC also establishes best practices and expectations.

3. Securities and Exchange Commission (SEC) <https://www.sec.gov/spotlight/cybersecurity>

[Commission Statement and Guidance on Public Company Cybersecurity Disclosures](#)

4. Health Insurance Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health Act (HITECH)

<https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

5. Family Educational Rights and Privacy Act (FERPA)

FERPA does not have specific breach notification requirements, however, it requires organizations to record every incidence of data disclosure. It does not require educational agencies and institutions to notify students if their records are stolen.

The US Department of Education created the Privacy Technical Assistance Center (PTAC) as a resource for cybersecurity issues in education.

PTAC's Data Breach Response Checklist:

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

6. General Data Protection Regulation (GDPR)

Starting May 25, 2018, the GDPR applies to companies that store or process the personal information of EU citizens in EU states. The regulation is consistent across all 28 EU states. Per Article 33 of the GDPR, organizations have 72 hours after learning of a data breach to report it.

<https://www.eugdpr.org/>

<https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>

7. PCI Data Security Standards (PCI DSS)

https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

RCW 42.56.590 - Personal information—Notice of security breaches.

RCW 43.43.856 - Divulging investigative information prohibited—Confidentiality—Security of records and files

RCW 42.56.230 - Personal information. (Effective until July 1, 2018.)

RCW 42.56.240 - Investigative, law enforcement, and crime victims (exempt from disclosure 2018)

RCW 42.56.27 - Financial, commercial, and proprietary information (exempt from disclosure 2018)

RCW 42.56.xxx other specific types of information exempt from disclosure

PPD#41

APPENDIX C - DOJ CTF COMPROMISED COMPUTER NETWORK INCIDENT WORKSHEET

1. Organization Information					
Organization Name:					
Organization Address:					
Name of Person Reporting:					
Name of Network Administrator:					
Name of CISO:					
Name of CIO/Executive Level Decision Maker:					
Date of Report:					
2. What type of network compromise occurred? (please select all that apply)					
<input type="checkbox"/> Reconnaissance	<input type="checkbox"/> Malware	<input type="checkbox"/> Data Exfiltration	<input type="checkbox"/> Other (please describe)		
3. What equipment has been impacted?					
Type:					
Manufacturer:					
Model Number:					
Serial Number:					
4. What operating system(s) was (were) installed on the equipment at the time of the intrusion?					
OS:		OS:		OS:	
Version:		Version:		Version:	
Time Zone:		Time Zone:		Time Zone:	
5. Are/Were software patches regularly installed?					
<input type="checkbox"/> Yes		<input type="checkbox"/> No		<input type="checkbox"/> Unknown	
6. Does your network utilize any virtual machines or cloud services?					
<input type="checkbox"/> Yes – If so, which ones?		<input type="checkbox"/> No		<input type="checkbox"/> Unknown	

7. Is remote connectivity enabled on your network?		
<input type="checkbox"/> Yes – Please select all that apply	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
<input type="checkbox"/> SSH – Please provide which version:		
<input type="checkbox"/> Telnet – Please provide which version:		
<input type="checkbox"/> RDP – Please provide which version:		
<input type="checkbox"/> VPN – Please provide which version:		
<input type="checkbox"/> Other – Please provide type and version:		
8. Does your organization use any web services?		
<input type="checkbox"/> Yes – Please list all services in use	<input type="checkbox"/> No	
9. Please list all domain names associated with your network.		
10. Please provide your server's DHCP address.		
11. Does your organization maintain DHCP logs?		
<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
12. Does your organization maintain web server logs?		
<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
13. Please provide your organization's network DNS address.		
Is it internal or external to your organization?		
<input type="checkbox"/> Internal	<input type="checkbox"/> External	<input type="checkbox"/> Unknown
14. Please list the range of your organization's IP addresses.		
Of these, how many does your organization own and/or use?		
15. Does your organization maintain any data backups?		
<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> Unknown

16. What terminal services are/were running on the impacted equipment?		
17. What ports are/were enabled on the impacted equipment?		
18. Does your organization own or operate any Wi-Fi access points?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
If so, are they active or passive?		
<input type="checkbox"/> Active	<input type="checkbox"/> Passive	
19. Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	
20. Are your employees informed of the limits of their acceptable use and privileges on your network?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
21. Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
22. Has your organization taken any steps to mitigate the impact of the intrusion?		
<input type="checkbox"/> Yes – if so, please describe	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
23. To the best of your ability, please quantify your estimated financial loss as a result of this incident.*		
Equipment Loss:		
Equipment Repairs:		
New Equipment:		
New Software:		
Employee Overtime:		
Consulting Costs:		
Reputation Degradation:		
Customer/Business Loss:		

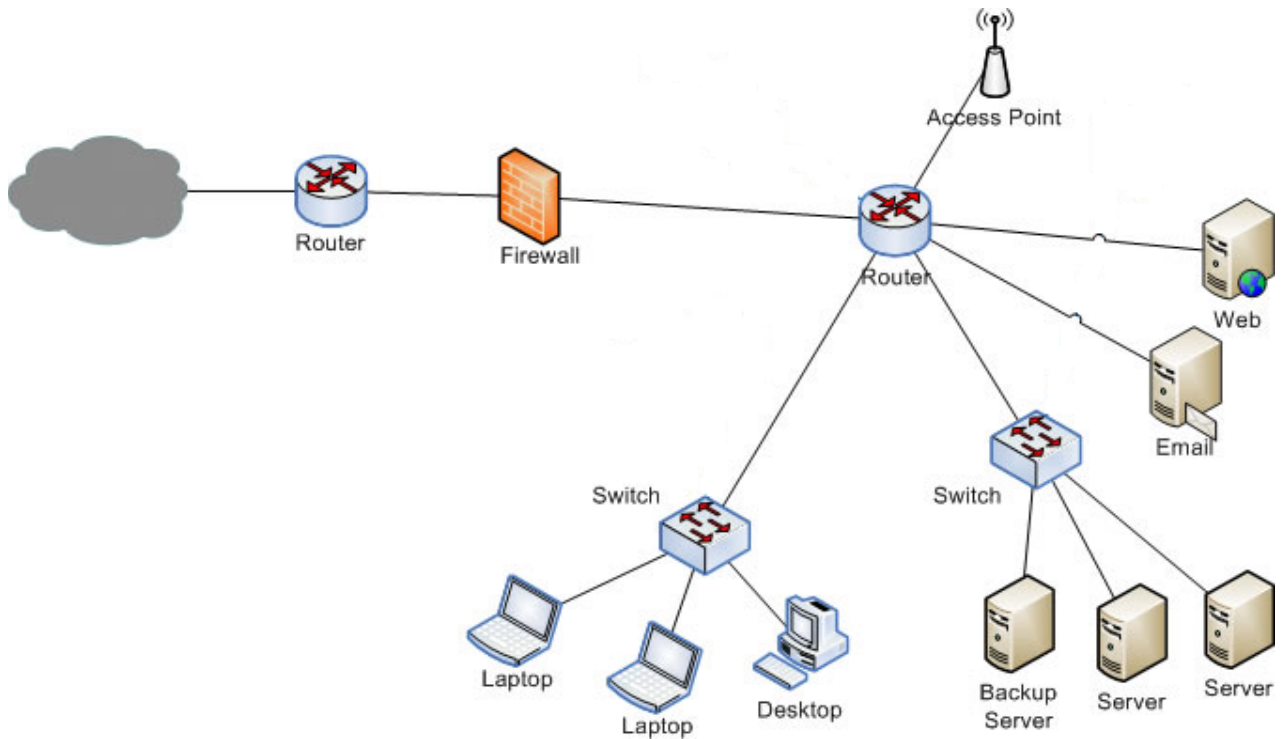
** We understand that an intrusion event can, regrettably, result in an array of costs and financial losses to your company. We also understand that it can sometimes take weeks or months to determine the full scope of those costs/losses. We seek that information, as you are able to provide it, because it is relevant to a criminal investigation. It is particularly important in determining the sentence that we will seek, assuming a successful prosecution and conviction.*

24. Please provide a diagram and narrative description of your network architecture and configurations that lists the location (city/state/country) of all servers and users on the network (see example).

25. Please provide the relevant usernames and passwords for all equipment impacted by the intrusion.

RESOURCES

1. Example diagram of network architecture and configurations.



2. Points of Contact

Federal Bureau of Investigation, Seattle – Cyber Task Force	206-622-0460
	seattle.ctf@ic.fbi.gov
United States Attorney’s Office, Western District of Washington	206-553-7970
United States Attorney’s Office, Eastern District of Washington	509-353-2767
Infragard	https://www.infragard.org
Internet Crime Complaint Center (IC3)	http://www.ic3.gov

NOTICE: This worksheet is intended to provide a baseline for reporting a computer network incident to the FBI. It is not exhaustive; however, it attempts to address the core elements of information that are most valuable to investigators in light of legal precedent and commonly used technologies. This document is not legal advice, and any best practices developed from it do not necessarily guarantee successful detection, investigation, and prosecution of adversaries.

APPENDIX D - ACRONYMS

ATF:	Alcohol,	Tobacco,	Firearms	(Bureau	of)				
AV:					AntiVirus				
CI/KR:	Critical		Infrastructure/Key		Resources				
CIO:	Chief		Information		Officer				
CIRCAS:	Cyber	Incident	Response	Coalition	and	Analysis	Sharing		
CISO:	Chief Information Security Officer								
CJIS:	Criminal		Justice	Information		System			
CONOPS:		CONcept		of		OPERationS			
CRDR:	Center	for	Regional	Disaster		Resilience			
CTF:		Computer		Task		Force			
DHCP:	Dynamic		Host	Configuration		Protocol			
DHS:	Department		of	Homeland		Security			
DNS:		Domain		Name		Service			
DOJ:		Department		of		Justice			
FBI:	Federal		Bureau	of		Investigation			
FERC:	Federal		Energy	Regulatory		Commision			
FERPA:	Family	Educational	Rights	and	Privacy	Act			
GDPR:	General		Data	Protection		Regulation			
HIPAA:	Health	Insurance	Portability	and	Accountability	Act			
HITECH:	Health	Information	Technology	for	Economic	and	Clinical	Health	Act
HSIN:	Homeland		Security	Information		Network			
IDS:				Detection		System			
IP:			Internet			Protocol			
ISAC:	Information		Sharing	Analysis		Center			
ISAO:	Information	Sharing	and	Analysis		Organization			
IT:			Information			Technology			
MTSA:	Maritime		Transportation	Security		Act			
NCCIC:	National	Cybersecurity	and	Communications	Integration	Center			
NCFTA:	National	Cyber-Forensics	&	Training		Alliance			
NERC:	North	American	Electric	Reliability		Corporation			
NIPP:	National		Infrastructure	Protection		Plan			

NIST: National Institute of Standards and Technology
 NRC: National Response Center
 NVIC: Navigation and Vessel Inspection Circular
 NWWARN: NorthWest Warning and Response Network
 OS: Operating System
 PCI DSS: Payment Card Industry Data Security Standard
 PD: Police Department
 PNWER: Pacific NorthWest Economic Region
 PTAC: Privacy Technical Assistance Center
 RDP: Remote Desktop Protocol
 SEC: Securities and Exchange Commission
 SLTGCC: State, Local, Tribal, and Territorial Government Coordinating Council
 SSH: Secure SHell (Protocol)
 TLP: Traffic Light Protocol
 TSA: Transportation Security Agency
 US-CERT: United States Computer Emergency Readiness Team
 USCG: United States Coast Guard
 VPN: Virtual Private Network
 WA State EMD or WSEMD: Washington State Department of Emergency Management
 WSFC: Washington State Fusion Center
 WSP: Washington State Patrol

APPENDIX E - SLTGCC CYBERSECURITY RESOURCE COMPENDIUM

The SLTGCC resource compendium lists some of the major references that can help build or strengthen an organization's cybersecurity program.

It is updated regularly. You can access the most recent version here:

<https://www.dhs.gov/publication/slgtgcc-cyber-resource-compedium>

APPENDIX F - WASHINGTON STATE PARTNER CYBER RESPONSE TEMPLATE

1. Introduction/Purpose

The following is a baseline version of a complete template that can be used to assess gaps you might have in your current cyber incident response plan. Some sections include examples while others simply outline the types of information that should be included. In all cases, it is highly recommended that you consider enlisting the assistance of qualified cyber incident response experts to develop the most appropriate and effective plan for your organization.

This playbook is meant to be a dynamic living document with relevant and up-to-date information to assist the Cyber Security Incident Response Team during a cyber security-related incident. This playbook contains the following resources:

- A quick start guide
- Incident Initiation checklist
- Removable checklists for each of the roles required in a response

Key response elements that should be included in a formal playbook will include but not be limited to:

- Incident Priority/classification guidelines
- Escalation guidance and contact information
- Communications plans and message templates
- Removable and/or electronic tracking/monitoring forms for:
 - Resource tracking
 - Event documentation
 - Communications tracking
 - Human resource management

2. Quick Start Guide

A Quick Start guide is a way to include the most important and relevant information in a concise format in order to allow responders to quickly gather and access resources and procedures at the beginning of an incident. It should include contact information for the following:

- Information Security On-Call
- Technical operations team
- Service Desk
- Incident Response team
- Internal Investigations/Audit
- Legal
- Facilities (Physical) Security

Cyber Security IR Team & Executive Emergency Contact Information

Fill in the table below with vital management and executive leadership who might need to be contacted during an event

Name	Position	Personal	Cell	Home Phone	Other
	CISO				
	Incident Response				
	Network Architect				

Insert any contact information for critical technical 3rd party vendors, e.g. Internet Service Providers; Managed security service providers; Cloud service providers, etc.

Important Links

Insert URL links to online tools, guides, or 3rd party systems that could be of assistance during an event, e.g. Virus Total; Threat Expert; etc.

Credit Card Notification Processes

This section is required by PCI DSS v.3.0 (Payment Card Industry Data Security Standards) – if your agency requires this section, contact a reliable expert to complete this section appropriately to your organization’s situation. If your organization is not required to comply with PCI DSS you can leave out this entire section.

Specific Response Process for Unauthorized Wireless Access Point

This section is required by PCI DSS v.3.0 (Payment Card Industry Data Security Standards) – if your agency requires this section, contact a reliable expert to complete this section appropriately to your organization’s situation. If your organization is not required to comply with PCI DSS you can leave out this entire section.

Engaging Law Enforcement

In some cases, an incident may benefit from, or require engagement with Law Enforcement. Even if they are unable to assist immediately – information you provide may assist them with Intelligence correlation and lead to prosecution or assistance in related cases, so it is always worthwhile to engage when possible.

If there is evidence that data has been stolen; there has been unauthorized access; or there is any threat to physical safety, the IR technician in charge or Incident Commander should check with Legal and, if given permission from the legal team, proceed to contact the appropriate Law Enforcement agency.

Engaging State Emergency Response Services

Through the Washington Military Department, Emergency Management Division, the Washington State Comprehensive Emergency Management Plan (CEMP), now includes a cyber annex (Annex D) -

<https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf>. A significant cyber incident is defined in this CEMP as an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture. This creates an opportunity and a new set of resources should your organization feels that there is an inherent or likely risk to critical infrastructure from the compromise you are experiencing.

Should you have reason to believe that the attack could expand in scope or affect other organizations, especially those that are critical to life, health, and the economic or physical well-being of our State, it is important to understand the method by which you engage the State's EMD.

State-level coordination of significant cyber incidents is triggered when the State Emergency Operations Center (SEOC) activates after receiving a request for assistance related to the incident. The pathway to the State is through your local emergency management personnel. Your local emergency management personnel will provide the coordination with state emergency management personnel.

They will need the same type of information as that which you would provide to law enforcement as noted above. They will also need documentation from legally responsible individuals in your organization that allows them to assign resources to assist you.

3. Escalation Triggers & outcomes

In this section create a set of steps that outline a typical scenario with its incident response triggers

4. Incident Initiation Checklist

Any event that significantly threatens the confidentiality, integrity or availability of the network and computer systems may be serious enough to initiate the Security Incident Response Procedure. The procedures to initiate that plan should be carefully considered for your organization.

5. Response Roles Checklists

The following roles have been developed by FEMA NIMS/ICS and follow NIST guidelines. Each of them should be carefully considered and defined based on your specific organization and its dependencies and priorities.

- Executive Oversight
- Incident Commander
- Communications Lead

- Command Liaison
- Operations Lead
- Logistics Lead
- Finance Lead

6. Incident Commander – Transfer of Command

In a cyber-security incident, the Incident Commander is drawn from responding Incident Response team members or possibly the first arriving stakeholder/authority at the scene.

However, it is often the case that command does not stay with the initial Incident Commander. The command should always be transferred to the most experienced and qualified person available regardless of that person’s employing agency or Department or Operational Unit.

The command may also be transferred when:

- A jurisdiction, Department, Operational Unit or agency is legally required to take command
- Changing command makes good sense (e.g. Priority or affected systems/ous have changed)
- The incident complexity changes
- There is a turnover of personnel on long or extended incidents
- Personal emergencies or other issues require a transfer of command
- Corporate executives direct a change in command

It is important to design a transfer of command procedure that meets your organization’s requirements.

7. Incident/Event Priority/Classification Detailed Guidelines

[Insert existing specific response procedures]

The following sections should be completed by your organization to best fit their needs and requirements

Definition of an incident

What defines an incident in your organization, e.g. as opposed to an everyday ‘event’. It is a good idea to list some examples here (with definitions), such as ‘viruses’, ‘worms’, ‘ransomware’, ‘phishing’, ‘compromise’, etc.

Incident/Event Priority Levels

Priority levels help determine the extent of response to security incidents by the Cyber Security Incident Response Team or an incident management team. These should be carefully considered and outlined in order to give your organization guidance on how to prioritize the response.

Roles and Responsibilities – Priority Level Matrix

Use a table structure to design an easy to understand and use a matrix that helps guide and inform your organization’s responders as to which parts of your organization should be involved in the response. As the example below shows, this correlates your priority levels with the roles you have defined

	Priority Level 1	Priority Level 2	Priority Level 3	Priority Level 4
	Insert synopsis of your priority 1 criteria here	Insert synopsis of your priority 2 criteria here	Insert synopsis of your priority 3 criteria here	Insert synopsis of your priority 4 criteria here
Incident Response Team	Involved	Involved	Involved	Involved
Incident Commander (IC)	Involved	Involved	Involved Dept Level only	N/A
Incident Scribe	Involved	Involved	N/A	N/A
Info Security Leadership	Informed &/or involved	Informed &/or involved	Informed &/or involved	Informed &/or involved
Service Desk	Informed &/or involved	Informed &/or involved	Informed &/or involved	Informed &/or involved
Leadership from other Operational Unit's	Informed &/or involved	Informed &/or involved	N/A	N/A
IT Leadership (CTO)	Informed &/or involved	Informed &/or involved	N/A	N/A
Legal Counsel	Informed &/or involved	Informed &/or involved	N/A	N/A
Fraud	Informed &/or involved	Informed &/or involved	N/A	N/A
Human Resources	Informed &/or involved	Informed &/or involved	N/A	N/A
Public Information Officer	Informed &/or involved	Informed &/or involved	N/A	N/A
Law Enforcement	&/or involved	&/or involved	N/A	

8. Monitoring and Response Tools

The following section should be completed to ensure you have adequate and efficacious procedures in place to use the monitoring and response tools available.

Basic Response Process

For any type of monitoring solution, there is a basic process which follows the more detailed description in the Incident Response Procedure document. Create a checklist for the responder/security analyst. Next list all of the response and monitoring tools you are currently using in your organization, e.g. antivirus, SIEM, file integrity, penetration testing, etc. and how they are deployed, accessed and what is the expected response process when they alert, etc.

9. High-Level Network Diagrams and Office Information

Insert network diagrams and office layout information/maps that could be of value during an incident.

10. Communications Plan

This plan defines the communications roles of all participants in a cyber-incident; the frequency and type of messages that should be used based on the Priority or escalation of an incident; and includes contact information for all possible participants.

Definitions

In this section, you should define any terms that will be used in the communications plan – below is a list of some possible terms:

- Application Owners
- Downtime List
- End Users
- Data Owners
- Executive Leadership
- Executive – Specific Operational Units

Messages and Channels

This section should include sample messages to be used as templates in the event of a system outage. If your organization is a complex infrastructure, the messages for end users may need to identify what is not available to them, rather than what the problem actually is.

The problem may not occur within systems but could be a problem with one of the access points to systems. If a remote access problem exists, there could be more than systems end-users impacted. Create templates for role-based emergency communications.

Appendix A – Communications Templates

In this appendix, you can insert actual templates that can be used by responders for communications. These should give examples of what information needs to be included. The following list are some possible templates you could create:

- Event Status Updates
- Event/Incident Close-out Final Report
- Final Report Template
- After Action Review
- General Communications

Other Communications Templates

In this section, you might create templates for communications regarding:

- Phishing
- Malware Outbreak
- Spoofing
- Ransomware
- Phone fraud

Appendix B – References

This section should be completed with links to reference materials that would be important during an event, e.g. Acceptable Use Policy; Security Incident Response Procedure; Breach Response Procedure (specific to PII data loss – may be owned by legal, audit or fraud); Corporate Incident Management, Business Continuity, Disaster Recovery Procedures; Disaster Recovery Site information.

Appendix C – Contact Lists

This section should be completed with specific contact information for all of the listed groups below or any others that might need to be contacted during an incident.

- Public Relations
- Human Resources
- End Users
- Corporate IT/Engineering/Network Notification Groups
- Application/Data or Operational Unit POC's
- Data Owners
- Operational Unit IT or Security Leads
- Executive Leadership
- Executive – Specific Operational Units

- Business Continuity
- Vendor contacts

You should consider obtaining Government Emergency Telecommunications Service (GETS) cards for your key response teams. This allows priority phone access for critical infrastructure providers such as hospitals during disasters and outages.

<https://www.dhs.gov/government-emergency-telecommunications-service-gets>

Appendix D – Preferred Providers

This section should be completed if you have contact information for 3rd party service providers to whom you can turn in the event you are unable to address a security event with your own resources.

This section should include sample Statements of Work (SOWs) and links to or copies of Master Service Agreements (MSAs).