**DRAFT**

**Washington Cybersecurity Situational Awareness CONOPS**

**(DRAFT v5.7)**

**Table of contents**

[**INTRODUCTION**](#_30j0zll)3

[1.1 Purpose](#_ibzf5cq5dk96) 3

[1.2 Background](#_3znysh7) 3

[1.3 Scope](#_2et92p0) 3

[1.4 Objectives](#_tyjcwt) 4

[**Current options and processes for reporting**](#_3dy6vkm)4

[2.1 Justification for a single point of contact reporting at the state and local level](#_swl7q7opfpig) 4

[2.2 US Coast Guard](#_1t3h5sf) 4

[2.3 Department of Homeland Security and Federal Law Enforcement](#_4d34og8) 5

[2.4 Local Law Enforcement and Intelligence – Washington State Fusion Center](#_2s8eyo1) 5

[**Local and Statewide Reporting Operations**](#_3rdcrjn)6

[3.1 OVERVIEW](#_26in1rg) 6

[3.2 CATEGORIES](#_lnxbz9) 6

[3.3 INCIDENT REPORTING TO WASHINGTON STATE FUSION CENTER (WSFC)](#_35nkun2) 7

[**Submission, Analysis, and Dissemination**](#_1ksv4uv)8

[4.1 Analysis of Agency Incident/Event Data](#_44sinio) 8

[4.2 Severity Rating](#_2jxsxqh) 9

[4.3 WSFC Products related to Cyber incident response](#_z337ya) 10

[4.3.1 WSFC After Action Reports](#_3j2qqm3) 10

[4.3.2 WSFC Monthly Trend Reports](#_1y810tw) 11

[4.4 On-site Incident Response Assistance to Agencies](#_4i7ojhp) 11

[4.5 Incident Escalation](#_2xcytpi) 11

[4.6 Notification of other related organizations, emergency management and law enforcement](#_1ci93xb) 11

[4.7 Communications](#_2bn6wsx) 12

[4.7.1 Communication During an Incident](#_qsh70q) 12

[4.7.2 Communication Guidelines](#_3as4poj) 12

[4.8 Regulatory Requirements](#_1pxezwc) 13

[**5.0 Securing and safeguarding information**](#_qg4g3fizmsjg)13

[5.1 Confidentiality](#_6ib2oblp1c7b) 13

[5.2 Outreach and education](#_cqbgpyj3j2py) 14

[**Appendix A Contact information**](#_49x2ik5) **Error! Bookmark not defined.**

[**Appendix B Regulatory requirements**](#_2p2csry)176

[**Appendix C DOJ Cyber Task Force (CTF) compromised Computer network incident worksheet**](#_tmrzb8hohxfx)19

# 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 cyber security 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 cyber security 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 (CIKR). 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 (CIKR) 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**

# 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’s (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 NCIC 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 are included in Appendix A.

However, it should be noted that while these are important and valuable resources for reporting and possibly for 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 note above, law enforcement, DHS NCIC, Washington State Emergency Management, The Cyber Incident Response Coalition & Analysis Sharing (CIRCAS), The National Cyber Forensics & Training Alliance (NCFTA) or other community resources.

# Local and Statewide Reporting Operations

## 3.1 OVERVIEW

It is the responsibility of any organization to combine the highest qualified and trained cyber security 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 resource | Within one (1) hour of discovery/detection. |
| **CAT 2** | **\*Denial of Service (DoS)** | An attack that *successfully* 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** | *Successful* 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 *successfully quarantined* by antivirus (AV) software. | Daily  Note: Within one (1) hour of discovery/detection *if* widespread across 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 system is classified, report within one (1) hour of discovery. |
| **CAT 6** | **Investigation** | *Unconfirmed* 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 about 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, 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.**

# 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 cyber security 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 to the 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. Minimal possibility of impact to other organizations. |
| High | 4 | Has impacted the organization. Likely impact to other organizations. |
| Crisis | 5 | Has had a severe impact on the operational capacity of the organization. Known or expected impact to 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 cyber security information with the organizations. Following this CONOPS the final state of the incident management process is 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 for 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 to 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 DEM 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 NCIC, 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 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?** |
| TLP:RED  TLP:RED  Not for disclosure, restricted to participants only. | 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. | 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. |
| TLP:AMBER  TLP:AMBER  Limited disclosure, restricted to participants’ organizations. | 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. | 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.** |
| TLP:GREEN  TLP:GREEN  Limited disclosure, restricted to the community. | 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. | 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. |
| TLP:WHITE  TLP:WHITE  Disclosure is not limited. | 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. | Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. |

## 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 update on training opportunities and to promote the conops.

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 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/NCIC - 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-thenations-  
  cybersecurity-1
* Law Enforcement Online Portal: <https://www.cjis.gov/CJISEAI/EAIController> or (888) 334-4536

1. NWWARN nwwarn.org
2. State of WA

* Office of Emergency Management - 800-258-5990,
* CISO - [cybersecurity@ocs.wa.gov](mailto:cybersecurity@ocs.wa.gov); 360–407–8700, 1–888–241–7597

1. 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 Commision (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>

1. 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 cyber security risks. The NVIC also establishes best practices and expectations.

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

[Commission Statement and Guidance on Public Company Cybersecurity Disclosures](https://www.sec.gov/rules/interp/2018/33-10459.pdf)

1. 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>

1. 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 cyber security 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>

1. 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>

1. 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: | | | | | |  | | | | | | | |
| 1. **What type of network compromise occurred? (please select all that apply)** | | | | | | | | | | | | | |
| ☐ Reconnaissance | | | ☐ Malware | | | | | ☐ Data Exfiltration | | | | ☐ Other (please describe) | |
|  | | | | | | | | | | | | | |
| 1. **What equipment has been impacted?** | | | | | | | | | | | | | |
| Type: | |  | | | | | | | | | | | |
| Manufacturer: | |  | | | | | | | | | | | |
| Model Number: | |  | | | | | | | | | | | |
| Serial Number: | |  | | | | | | | | | | | |
| 1. **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: | |  |
| 1. **Are/Were software patches regularly installed?** | | | | | | | | | | | | | |
| ☐ Yes | | | | ☐ No | | | | | ☐ Unknown | | | | |
| 1. **Does your network utilize any virtual machines or cloud services?** | | | | | | | | | | | | | |
| ☐ Yes – If so, which ones? | | | | | ☐ No | | | | | ☐ Unknown | | | |
|  | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Is remote connectivity enabled on your network?** | | | | | | | |
| ☐ Yes – Please select all that apply | | ☐ No | | | ☐ Unknown | | |
| ☐ SSH – Please provide which version: | | | | | | | |
| ☐ Telnet – Please provide which version: | | | | | | | |
| ☐ RDP – Please provide which version: | | | | | | | |
| ☐ VPN – Please provide which version: | | | | | | | |
| ☐ Other – Please provide type and version: | | | | | | | |
| 1. **Does your organization use any web services?** | | | | | | | |
| ☐ Yes – Please list all services in use | | | | ☐ No | | | |
|  | | | | | | | |
| 1. **Please list all domain names associated with your network.** | | | | | | | |
|  | | | | | | | |
| 1. **Please provide your server’s DHCP address.** | | | | | | | |
|  | | | | | | | |
| 1. **Does your organization maintain DCHP logs?** | | | | | | | |
| ☐ Yes – If so, where? | | | ☐ No | | | ☐ Unknown | |
|  | | | | | | | |
| 1. **Does your organization maintain web server logs?** | | | | | | | |
| ☐ Yes – If so, where? | | | ☐ No | | | ☐ Unknown | |
|  | | | | | | | |
| 1. **Please provide your organization’s network DNS address.** | | | | | | | |
|  | | | | | | | |
| **Is it internal or external to your organization?** | | | | | | | |
| ☐ Internal | ☐ External | | | | | | ☐ Unknown |
| 1. **Please list the range of your organization’s IP addresses.** | | | | | | | |
|  | | | | | | | |
| **Of these, how many does your organization own and/or use?** | | | | | | | |
|  | | | | | | | |
| 1. **Does your organization maintain any data backups?** | | | | | | | |
| ☐ Yes – If so, where? | | | ☐ No | | | ☐ Unknown | |
|  | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **What terminal services are/were running on the impacted equipment?** | | | | | | | |
|  | | | | | | | |
| 1. **What ports are/were enabled on the impacted equipment?** | | | | | | | |
|  | | | | | | | |
| 1. **Does your organization own or operate any Wi-Fi access points?** | | | | | | | |
| ☐ Yes | | ☐ No | | | | ☐ Unknown | |
| **If so, are they active or passive?** | | | | | | | |
| ☐ Active | | | | ☐ Passive | | | |
| 1. **Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee?** | | | | | | | |
| ☐ Yes | | | | | ☐ No | | |
| 1. **Are your employees informed of the limits of their acceptable use and privileges on your network?** | | | | | | | |
| ☐ Yes | | ☐ No | | | | ☐ Unknown | |
| 1. **Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?** | | | | | | | |
| ☐ Yes | | ☐ No | | | | ☐ Unknown | |
| 1. **Has your organization taken any steps to mitigate the impact of the intrusion?** | | | | | | | |
| ☐ Yes – if so, please describe | | | ☐ No | | | | ☐ Unknown |
|  | | | | | | | |
| 1. **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.*** | | | | | | | |
| 1. **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).** | | | | | | | |
|  | | | | | | | |
| 1. **Please provide the relevant usernames and passwords for all equipment impacted by the intrusion.** | | | | | | | |
|  | | | | | | | |

**RESOURCES**

|  |  |  |
| --- | --- | --- |
| 1. **Example diagram of network architecture and configurations.** | | |
| C:\Users\JRieth\Desktop\network example.png | | |
| 1. **Points of Contact** | |
| Federal Bureau of Investigation, Seattle – Cyber Task Force | 206-622-0460 |
| [seattle.ctf@ic.fbi.gov](mailto: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.***