Cyber Disruption Response Plan

Hawai‘i Office of Homeland Security

MARCH 2022 |

AUTHORITY AND ADOPTION LETTER

EXECUTIVE SIGNATORY PAGE

The most fundamental function of government is providing for the safety and welfare of the public. An effective Cyber Security program is essential to ensuring the state of Hawai'i fulfills this responsibility when our state is threatened or impacted by cyber disruption.

The State of Hawai'i ***Cyber Disruption Response Plan (CDRP)*** establishes the framework our State Government will use to organize and coordinate its response activities for a coordinated approach to responding to cyber disruptions that impact our state.

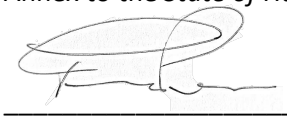
This CDRP, an Incident Annex to the State Emergency Operations Plan, outlines organizations, actions, and responsibilities of state and county departments and agencies and identifies how they will work together to ensure the state is prepared to execute a well-coordinated, timely and consistent cyber disruption response. It is intended to be a living document that evolves and improves as the outcomes of ongoing planning efforts, exercises, and real-world events are incorporated.

This plan is written in accordance with Hawai'i Revised Statutes (HRS) Chapters 128A (Homeland Security) and 128B (Cybersecurity) and applies to all state departments including agencies, offices, institutions of higher education, commissions, boards, and councils. This ***CDRP***/Annex does not direct the emergency operations of local governments, federal agencies, private sector, or non-governmental organizations. However, it does provide a reference for their response plans, procedures, and actions.

It is important to emphasize that responsibility for the initial response and management of an emergency rests with the affected entity(ies), to include local jurisdictions. The state's response supports state government efforts when additional resources are required or not available within the affected entity. This plan describes how those state resources will be activated, requested, and coordinated to complement response efforts.

This document is maintained by the Hawai'i State Office of Homeland Security (OHS) with input from state and county departments and agencies.

I hereby promulgate and adopt the State of Hawai'i ***Cyber Disruption Response Plan*** as an Incident Annex to the *State of Hawai'i Emergency Operations Plan***.**



_____

Frank J. Pace, Administrator
Office of Homeland Security
Hawai'i Department of Defense
MAR 2, 2022

RECORD OF APPROVAL

Approval #	Approval Date	Approval Authority	Type of Approval
2			
1			

RECORD OF CHANGES

Change Number	Date of Change	Page or Section Changed	Summary of Change	Authorization Signature	Date of Signature
1					
2					
3					
4					
5					
6					
7					

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

In Hawai'i Revised Statutes (HRS) Chapter 128A (Homeland Security) the state legislature; finding existing and increasing possibility of attacks (defined to include cyber) of unprecedented size and destructiveness and to ensure adequate preparation to deal with such attacks; preserve the lives and property of the people of the State; and protect the public peace, health, and safety; created the Hawai'i State Office of Homeland Security (OHS). Chapter 128A outlines the OHS responsibilities to include preparing comprehensive plans and programs for homeland security. HRS Chapter 128B (Cybersecurity) Cybersecurity Coordinator were absorbed into the OHS when that position was abolished. Under these collective authorities, the OHS, in coordination with appropriate entities and individuals, develops, regularly updates, maintains, and exercises adaptable response plans to address cybersecurity risks, including significant cyber incidents (***disruptions***) contemplated in this ***Cyber Disruption Response Plan***.

The ***Presidential Policy Directive (PPD)-41: U.S. Cyber Incident Coordination*** set forth principles governing the Federal Government's response to any cyber incident, provide an architecture for coordinating the response to significant cyber incidents, and required DHS to develop a ***National Cyber Incident Response Plan (NCIRP)***. This ***CDRP*** follows the ***NCIRP*** concept as part of the broader National Preparedness System and establishes the framework for a whole-of-Nation[1] approach to responding to a cyber incident ***(disruption)*** in the State of Hawai'i. This whole-of-Nation concept focuses efforts and enables the full range of stakeholders—the private and nonprofit sectors (including private and public owners and operators of critical infrastructure), state and local governments, and the Federal Government—to participate as full partners in incident ***(disruption)*** response and both includes and strongly relies on public and private partnerships to address major cybersecurity risks.

Any organization with sensitive data can be attacked, regardless of size or sector. And as the threat landscape evolves and adversaries deploy tactics, techniques, and procedures, security professionals and stakeholders must also adapt their security plans. Depending on the situation, a targeted attack may involve the theft of source code, valuable intellectual property, negotiation data or general operational disruption. Companies and governments need to be prepared to identify, respond to, and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster response or recovery plan.[2]

States are now developing disruption response plans to respond to a significant cyber incident — cyberattacks that "pose demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of

[1] The whole-of-Nation approach also encompasses a wide range of new and existing public and private partnerships to leverage as a platform in working towards managing cybersecurity threats and hazards to critical infrastructure.
[2] CrowdStrike Services. (undated). *You've Been Breached – Now What?: How to Respond to a Worst-Case Cyber Scenario.* Accessed September 10, 2021 at: WhitepaperIncidentResponse.pdf (crowdstrike.com)

[the public]."[3] These plans differ from incident response plans because they require multiple agencies to coordinate activities and implement traditional emergency management and homeland security operations. Like a Category 5 hurricane, states realize that they have a role in mitigating the impact of such a scenario and are solidifying those roles and responsibilities in cyber disruption response plans.[4]

1.2 SCOPE

This ***CDRP*** describes the framework for state cyber disruption response and short-term recovery coordination among multiple state, local, and federal agencies and private entities with critical computer information or operational systems or cyber response assets or capabilities. This plan provides a framework for a cyber response and short-term recovery, including the establishment of a Cyber Unified Coordination Group (C-UCG) and an outline of the C-UCG's roles and responsibilities in the coordination of rapid identification, information exchange, response, and short-term recovery and remediation to mitigate the damage caused by either a deliberate or unintentional significant cyber incident. Activities conducted pursuant to this ***CDRP*** are compliant with the National Incident Management System (NIMS) and take place within state and local planning and incident command structures, complement existing plans and procedures.

1.2.1 Policy

Procedures for utilization, control and use will incorporate and/or consider operational priorities that include, but are not limited to, the protection of life, public health and safety, property protection, environmental protection, restoration of essential utilities, restoration of essential program functions, and coordination as appropriate.

The governor or designee may authorize and direct the use of state resources to provide support and assistance to disruption handling efforts for internal and external organizations after consideration of both priority of need and cost.

In situations where an imminent threat exists to life safety, or an identified need for the protection of critical infrastructure and environment exists, priorities established within the ***Hawai'i Emergency Operations Plan (HI-EOP)*** take precedence over agency priorities.

1.2.2 Definitions

Asset response activities include furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities, and assessing their risk to the same or similar vulnerabilities.

[3] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

[4] National Governor's Association. (2019, July). *Issue Brief: State Cyber Disruption Response Plans.* Accessed September 10, 2021 at: IssueBrief_MG.pdf (nga.org)

A ***cyber-attack*** is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity."[5] Cyber-attacks are intentional and can be carried out by individuals, organizations, or government entities. They range from unsophisticated attempts made by amateur hackers using existing computer scripts, to sophisticated attempts sponsored or carried out by international governments. There are many types of attacks in between these extremes. "Hacktivists" are individuals or groups who use hacking to promote their social or political ideology. Additionally, threat agents may use ransomware, malicious software designed to restrict access to a system or data until a sum of money is paid. Espionage and data theft could degrade public safety, expose the State or its counties to financial risk and the public to identity theft. In 2019, Hawai'i state victims of internet crimes lost over $9 million, mostly through fraud schemes.[6] Tactics used in cyber-attacks are always changing and becoming more sophisticated. The U.S. Department of National Intelligence's 2018 Worldwide Threat Assessment states that U.S. adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.[7] The report goes on to say that while cyber-attack as a foreign policy tool has been mostly confined to low-level attacks, these state-sponsored actors have been testing more aggressive tactics in recent years. In 2016, the Department of Homeland Security stated that they were confident that Russia was responsible for hacking the Democratic National Committee (DNC) and leaking thousands of DNC emails during the presidential election.[8]

A ***cyber-crime*** is any type of illegal activity that takes place via digital means. Data theft is one of the most common types of cyber-crime, but cyber-crime also includes a wide range of malicious activity such as cyberbullying or planting worms or viruses. The top three crime types reported by victims in 2019 were phishing/vishing/smishing/pharming, non-payment/non-delivery, and extortion.[9]

A ***cyber incident*** is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon." [10]

---

[5] Check Point Software Technologies LTD (undated). *What Is a Cyber Attack?* Accessed September 10, 2021 at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

[6] FBI Internet Crime Complaint Center data. (Undated). Accessed September 10, 2021 at: https://www.ic3.gov/Media/PDF/AnnualReport/2019State/StateReport.aspx#?s=14

[7] Coats, Daniel R. Office of the Director of National Intelligence. (2019, January). *Worldwide Threat Assessment of the US Intelligence Community.* Accessed September 10, 2021 at: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[8] U.S. Department of Homeland Security. (2016, October). *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security.* Accessed September 10, 2021 at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[9] U.S. Department of Homeland Security. (2020, February). *FBI Releases IC3 2019 Internet Crime Report*. Accessed at: https://us-cert.cisa.gov/ncas/current-activity/2020/02/12/fbi-releases-ic3-2019-internet-crime-report

[10] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

A ***denial-of-service*** attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.[11]

An ***Electromagnetic Pulse (EMP)*** is an intense burst of electromagnetic energy resulting from natural (e.g., solar storms) or human (e.g., nuclear or pulse-power device) sources. Both types can destroy or damage unshielded electrical and electronic equipment. Solar storms can induce extreme currents in wires, disrupting power lines, and causing wide-spread blackouts to the communication cables that support the internet.[12] There is still much we do not understand about how effective nuclear weapons are as EMP weapons, especially lower yield bombs that terrorists or small states would probably use. The scale and scope of damage caused by an EMP could vary considerably based on the type of device, and the altitude and latitude of the detonation. A nuclear device detonated at high altitudes (30-400 km) could generate an EMP with a radius of effects from hundreds to thousands of kilometers.[13] While it could disable electrical and electronic systems in general, it would pose the highest risk to electric power systems and long-haul communications.[14]

Indirect Effect. Other hazards or human error can have effects on digital networks and information. Power outages can create cyber disruptions. In 2006 many parts of Seattle lost power for days. Many individuals and small businesses had trouble powering computers and mobile devices. As computers become our primary tools for gathering information and communicating, their loss can endanger public safety and welfare. If the power goes out and fuel delivery to generator sites is impaired, bigger sites like communications hubs and data centers could go down causing disruption if they are not adequately backed up. Additionally, communications equipment often sits under high-powered sprinklers. If there was a fire in one of these buildings or a sprinkler head was knocked off, it could damage equipment and cause disruptions to communications. Human error can also play a role in cyber-related incidents. An unintentional release of sensitive digital information presents a potential threat to personal and financial security.

[11] U.S. Department of Homeland Security. (2019, November). *National Cyber Awareness* System. Accessed September 10, 2021 at: https://us-cert.cisa.gov/ncas/tips/ST04-015

[12] National Aeronautics and Space Administration. (2009, January). *NASA-Funded Study Reveals Hazards of Severe Space Weather.* Accessed September 10, 2021 at: https://www.nasa.gov/topics/solarsystem/features/spaceweather_hazard.html.

[13] U.S. Department of Energy. (2017, January). *U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan*. Accessed September 10, 2021 at: https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf

[14] Ibid.

Intelligence support activities include information to better understand the cyber incident and existing targeted diplomatic, economic, or military capabilities to respond and share threat and mitigation information with other potential affected entities or responders.

Physical Damage. Cyber disruptions can also happen as secondary effects from other kinds of hazards. Earthquakes, floods, and fires can destroy computer and network equipment. Most of the time the effects are limited due to the availability of back-up systems and the ability to route networks around problem sites. Nevertheless, if a significant network node goes down the effects could be wide-spread and possibly prolonged. Communications can be disrupted by physical damage to copper or fiber cables, or radio equipment located on buildings. Damage to cables has accidentally occurred during construction or repaving projects, causing temporary internet and phone outages for thousands of customers.

A ***significant cyber incident*** is defined as a "a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[15]

Threat response activities during a cyber incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities.

1.2.3 Relationship to Other Plans

The ***Cyber Disruption Response Plan (CDRP)*** is an Annex to the ***HI-EOP*** which is the state's all-hazards plan that establishes the framework used to coordinate the state response to, and recovery from, emergencies and disasters. The ***CDRP*** Annex addresses unique planning, response, and short-term recovery requirements for cyber disruption (a significant cyber incident) but is not intended to duplicate or alter the response concepts outlined in the ***HI-EOP.***

Additionally, the ***Cyber Incident Response Plan (CIRP)*** is an Appendix to the State of Hawai'i ***CDRP***. The ***CIRP*** addresses unique planning and response requirements for a state Information Technology (IT) enterprise cyber incident but is not intended to duplicate or alter the response concepts outlined in this ***CDRP.***

[15] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

2. SITUATION AND ASSUMPTIONS

2.1 SITUATION OVERVIEW

Cyber incidents may take many forms:

- An organized attack;
- An uncontrolled exploit, such as a virus, worm, or Denial of Service which has a widespread impact on public safety;
- A natural disaster with significant cyber consequences;
- Other incidents causing extensive damage to critical infrastructure;
- Inadequate or improper IT infrastructure maintenance, security, and/or design.

In addition, an incident can be a "false positive" where no actual damage or danger is present, but an investigation is needed to reach that conclusion.

Cyber-attacks, cyber-crime, and unintentional incidents caused by natural disaster or human error can also lead to large scale or long-term disruption of service. The results of these events can lead to the loss of mission critical information, unavailability of information systems that support public sector internet, critical infrastructure, public health, economic institutions, and other organization that sustain and provide critical services to State Hawai'i residents and visitors. Cyber threats can endanger vital control systems for other infrastructure such as electricity generation, transmission, and distribution.

Information technology service providers within Hawai'i play a vital role in cyber incident response because the public sector provides the backbone for IT systems and are the most predominant owners/operators of the critical infrastructure and performers of critical functions that IT systems support. Federal, State, and local Government computer assets are all connected in varying degrees to privately administered critical communications infrastructure providers. It is essential that these providers be integrated into the coordination and decision-making processes in this ***CDRP.***

Cyber incidents have the potential to overwhelm or disable government and private sector resources. The computer networks utilized by State of Hawai'i government agencies and those that support critical infrastructure provide critical services, including those that support public safety and public health. Technical staff within organizations must keep up with current technologies as cyber threats change, and the training can be expensive. Redundancy must continue to be built into computer networks, and continuity of operations plans for all governmental and critical infrastructure organizations must be maintained and tested.

2.1.1 THREAT ANALYSIS

Because of the relative lack of cybersecurity expertise and their need to stay operational state and local governments have become a favored target of cybercriminals, especially ransomware operators, because small government agencies are more likely to pay to recover from a ransomware attack.[16]

Since 2017, attacks – which the report defines as targeted instances of intrusion, fraud, or damage by malicious cyber actors rather than discovery of insecure databases or accidental online leaks – rose an average of almost 50%, likely only a fraction of the true number.[17]

Ransomware is the main way municipal assets are attacked. What is more concerning than the growing number of attacks, however, is the increase in how much bad actors demand in ransom. Average ransom demands rose from a monthly average of $30,000 to nearly half a million dollars, with total monetary value of ransom demands reaching into the millions.[18]

Even when cities do not pay, the costs can be staggering. For instance, the 2019 ransomware attack on Baltimore cost the city more than $18 million in damages and remediation.[19]

Looking forward, a recent trends outlook highlighted eight trends anticipated for 2021:[20]

- Next-Generation Extortion and Evolution in Malware Business Models
- Supply Chain Attacks via Cloud-Hosted Development Environments
- AI, Evasion, and Theft
- Parcel and Shipping as Critical Infrastructure
- Mandated Contact Tracing Apps May Open Doors for Large-Scale Cyber Attacks
- Cybercriminals Will Likely Capitalize on Rapid U.S. Telehealth Adoption
- 5G to Expand the Attack Surface for Industrial IOT
- 5G to Increase Security Pressure on Mobile Hotspots

Hawaii's cyber security risk profile trends medium to high:

- **People:** There is increasing possibility of attacks that paralyze critical infrastructure sectors/facilities, creating far-reaching effects statewide, impacting most, if not all, of the population.
- **Property:** Damages can vary wildly but are most likely going to be localized. While statewide, risk to properties is minimized due to the state's archipelago nature, property impacts from

[16] DARKReading. (2020, June). *Local, State Governments Face Cybersecurity Crisis.* Accessed November 12, 2020 at: https://www.darkreading.com/attacks-breaches/local-state-governments-face-cybersecurity-crisis/d/d-id/1338010#:~:text=Already%2C%20government%2Dfocused%20companies%20have,state%20and%20local%20government%20clients.&text=In%202019%2C%20more%20than%20104,threat%20intelligence%20firm%20Recorded%20Future.

[17] BlueVoyant. (2020, August). *State and Local Government Security Report.* Accessed November 12, 2020 at: https://www.bluevoyant.com/state-and-local-gov-security-report

[18] Ibid.

[19] GCN. (2020, September). *Cyberattacks on state, local government up 50%.* Accessed November 12, 2020 at: https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx.

[20] Booz-Allen-Hamilton. (2020). *2021 Cyber Threat Trends Outlook.* Accessed November 12, 2020 at: https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/cyber-threat-trends-outlook-2021.pdf

cyber incidents is increasingly fluid across a broad attack surface implicating multiple sectors and/or multiple victims.

- **Environment:** Cyber intrusions and attacks can pose a significant pollution liability risk with potential to cause damage to human health and the environment from catastrophic spills, waste discharges, and air emissions. These events can cause fires, explosions and hazardous material releases that result in bodily injury, property damage, and environmental remediation.
- **Continuity / Operations:** A cyber-attack against State or county government or critical infrastructure that responsible responding organizations are dependent upon (i.e., electricity, communications, transportation) could completely cripple State and local government and/or state and county emergency management program operations until systems could be restored.

2.1.2 VULNERABILITY ANALYSIS

Based on analysis of FBI cyberattack data, states' who report to the National Governor's Association for spending on cybersecurity and how safe each state's election systems are, Hawai'i ranks at the top of those states at most risk of cyberattacks.[21] While that analysis was looking across all of the state and through the lens of election systems and not focused on the state IT enterprise, like other states in the nation, the State of Hawai'i continues to work to increase their cybersecurity posture with limited resources.

At the time of the writing of this plan, the Coronavirus Disease that appeared in 2019 (COVID-19) has dominated every state's leadership agenda for most of 2020 and 2021, and that is true for the State of Hawai'i IT enterprise. But even before, the enterprise was dealing with the ongoing struggle for adequate funding, challenges of cyber staffing, and ever-evolving cyber threats. COVID-19 acted as a major accelerant, increasing the urgency of efforts of critical importance.

Telework was already happening, but on a smaller scale. As of this writing, remote work is the dominant operating principle of state government. Additionally, there was more data to protect due to unprecedented demand for government services such as unemployment compensation and other digital services. Some of these changes are likely to become permanent, continuing to strain against the state's cybersecurity vulnerabilities:

- Lack of sufficient cybersecurity budget
- Inadequate cybersecurity staffing
- Legacy infrastructure and solutions to support emerging threats
- Lack of dedicated cybersecurity budget
- Inadequate availability of cybersecurity professionals

When looking more broadly, Hawaii's cyber security vulnerability profile trends medium to high:

[21] Security.org. (2019, August). *What States Are at Highest Risk for Cyberattacks.* Accessed November 12, 2020 at: https://www.security.org/resources/states-highest-risk-cyberattacks/.

- **People:** Depending on the type of attack and its target, vulnerable populations could be specific agencies/organizations or groups, but can just as readily encompass multiple sectors, critical functions, and create vulnerable populations with their impacts.
- **Property:** Industrial control systems such as water treatment facilities/pipelines and transportation systems are vulnerable to cyber-attack. All critical infrastructure sectors are (and increasingly so) vulnerable to ransomware attacks that can render systems inoperable temporarily or permanently, necessitating complete replacement.
- **Environment:** All ecosystems that have interface with cyber-reliant or cyber-enabled human infrastructure systems, including marine and air, carry the potential to sustain environmental impacts from and are vulnerable to cyber-attacks.
- **Continuity / Operations:** Plans calling for documentation and system backups provide minimal continuity for state/county and their emergency management programs without significant delay; however, these plans and this mitigation approach are not universal to all government organizations that have responsibilities in supporting emergency management and that inhibits those operations in the state. Additionally, operational effectiveness will be impacted more so should critical infrastructure sectors also experience direct or cascading impacts from a cyber incident.

In the national context, vulnerability for the State of Hawai'i also comes in the form of a significant partner and neighbor on the islands. The U.S. Department of Defense's (DoD's) U.S. Indo-Pacific Command (USINDOPACOM) Headquarters and all its supporting service component's headquarters on Oahu and has several other installations strewn amongst the island chain. This cluster of military capability is an attractive target for hostile nation-states and other actors. In the event of a cyber incident, both the U.S. military and the state government could face devastating disruption to their IT enterprises as well as other life-sustaining services.

2.2 ASSUMPTIONS

- Affected entities may not have operational situational awareness and/or control or be responsible for incident response activities based on applicable laws, statutes, and authorities.
- Notification to state agencies regarding cyber incidents will be carried out in accordance with this ***CDRP***.
- The ***CDRP*** is based on current Hawai'i Revised Statues; any further required/desired authorities or similar would require additional statues to be developed.
- Due to limits on situational awareness, activation the Emergency Operations Plan/Emergency Operations Center will be a decision point based on the nature and awareness of the extent of the disruption.
- There will not be sufficient cyber incident response capability at the affected entity or within the state.

- Mutual aid agreements and pre-scripted missions will be required to meet response requirements for a significant cyber incident.
- Affected entities will follow their relevant response plans, including consultation with any pre-arranged no cost retainer legal and breach consulting experts and cyber security and forensic analysis companies, to take appropriate actions such as terminating unauthorized access, minimizing damage, analyzing scope and depth of intrusion, and preservation evidence.
- The effects of a significant cyber incident may be widespread affecting multiple entities, both public and private, and have local and state impacts, for a period lasting beyond two weeks.
- Without help from residents, professionals, and private-sector organizations, the state government alone will not have the scale to improve the overall cybersecurity of Hawai‘i.

3. CONCEPT OF OPERATIONS

3.1 PREPARATION

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.[22]

A significant cyber incident (e.g. Ransomware outbreak, Denial of Service attacks, etc.) may create effects of such magnitude against information systems, resources, and operations and across multiple entities simultaneously or near-simultaneously such that it may require the Governor to declare an emergency and activate the necessary resources to respond to and perform short-term recover to stem potential damage and/or loss of confidentiality, integrity, availability, reputation, and public trust.

Upon activation, all applicable National, State, local, interjurisdictional, and private sector significant cyber incident response organizations (or functional equivalent) should provide cooperation and coordination with the designated entities, affected agency(ies), and appointed officers in response and short-term recovery efforts. All parties should identify and prioritize the appropriate means to:

- Communicate securely and effectively with designated response/recovery entity members (e.g., situation/war room); contact information is crucial.
- Coordinate the use of response and short-term recovery resources (e.g., analysis tools, mitigation software, etc.) and personnel management.
- Track and monitor the incident response and short-term recovery activities (e.g., incident tracking/ticketing mechanisms, etc.) until closure.

3.2 DETECTION, ANALYSIS, AND NOTIFICATION

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies.[23]

3.2.1 Detection

Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may

[22] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[23] Ibid

be occurring now. Most attacks do not have any identifiable or detectable precursors from the target's perspective. If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.[24]

3.2.1 Impact Analysis

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis because of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as:[25]

Functional Impact of the Incident. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.

Information Impact of the Incident. Incidents may affect the confidentiality, integrity, and availability of the organization's information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

Recoverability from the Incident. The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances, it is not possible to recover from an incident and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to recover from an incident and carefully weigh that against the value the recovery effort will create, and any requirements related to incident handling.

3.2.2 Notification and Activation

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber-attacks that damage computer systems can cause lasting harm to anyone engaged in

[24] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[25] Ibid

personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.[26]

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery.[27]

When supporting affected entities, the Hawai'i State Government, and the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice.

When to Report

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Hawai'i State and Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact many victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

[26] U.S. Department of Homeland Security. (Undated). *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. Accessed October 28, 2021 at: https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
[27] Ibid

How to Report

If there is an immediate threat to public health or safety, initial notice should always be to 911.

Private sector entities experiencing cyber incidents within the state of Hawai'i are encouraged to report to the Hawai'i State Fusion Center, local field offices of federal law enforcement agencies, their sector specific agency, and any of the applicable federal agencies listed section 4.3. The entity receiving the initial report will coordinate with other relevant state and federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident as described above. The affected entity is responsible for internal and support partner notifications, alerts.

Key State Point of Contact:

Hawai'i State Fusion Center (HSFC)

HSFC: (808) 369-3589 or HSFC@hawaii.gov

Report suspected or confirmed cyber incidents, intrusions, or attacks, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity.

Report cyber-enabled crime, including digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

Key Federal Points of Contact:

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov
United States Computer Emergency Readiness Team: http://www.us-cert.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
Internet Crime Complaint Center (IC3): http://www.ic3.gov

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

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):
http://www.secretservice.gov/contact/field-offices

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form
HSI Field Offices: https://www.ice.gov/contact/hsi
HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes

Report cyber-enabled crime, including digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

United States Coast Guard (USCG)

USCG Sector Honolulu: 808-842-2600
National Response Center: 800-424-8802

Report, without delay, cyber incidents and suspicious activities impacting security and/or safety of maritime ports, vessels, and waterways.

COORDINATION OF PUBLIC INFORMATION. Reference the State Emergency Operations Plan for details regarding coordination of this element of notification concerning information to be shared publicly. Alert and warning are not mandatory; unless required by law, statute or regulatory directed. If required, the State of Hawai‘i through the C-UCG and related response mechanisms will coordinate with affected entities to assist with meeting this requirement.

ACTIVATION OF THE STATE EMERGENCY OPERATIONS CENTER (SEOC). The need to activate the State EOC is based on the scope, scale, and complexity of a threatening or occurring cyber incident. OHS will notify HSFC regarding notifications, alerts, and/or warnings to stakeholders, key-decision makers, and

executive officers. OHS will also provide advice and recommendations to the Homeland Security Advisor regarding the need or desire to stand up a C-UCG, which would also include incident notification to the State EOC.

Upon State EOC notification of a significant cyber incident, the level of SEOC activation will be determined by the Administrator of Emergency Management, Executive Officer, or Operations Section Chief in conjunction with the decision to activate a C-UCG.

3.3 INCIDENT HANDLING

3.3.1 Containment

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early while handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. Containment strategies vary based on the type of incident.[28]

Evidence Gathering and Handling - While the primary reason for gathering evidence during an incident by the affected entity is to resolve the incident, it may also be needed for legal proceedings, particularly when individual incidents are part of a larger ***significant cyber incident***. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In addition, evidence should be always accounted for; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence.[29]

Identifying the Attacking Hosts - During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers in affected entities should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the operational impact.[30]

[28] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[29] Ibid.

[30] Ibid.

3.3.2 Eradication

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.[31]

3.3.3 Recovery

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.[32]

For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.[33]

3.4 POST-INCIDENT ACTIVITY

One of the most important parts of incident response is also the most often omitted: learning and improving. Each significant incident response must enable evolution that reflects new threats, improved technology, and lessons learned. To this objective, the C-UCG will coordinate and host a "lessons learned" meeting with all involved parties after a significant cyber incident. The meeting should be held within several days of the end of the significant cyber incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did responding organizations and their staff perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the organizations do differently the next time a similar incident occurs?

[31] Ibid.
[32] National Institute of Standards and Technology. (2012, August). *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology.* Accessed September 10, 2021 at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
[33] Ibid.

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

4. ROLES AND RESPONSIBILITES

4.1 HAWAIʻI STATE GOVERNMENT

4.1.1 STATE DEPARTMENT OF DEFENSE

4.1.1.1 OFFICE OF HOMELAND SECURITY

- Ensure that it has the standing capacity to execute its role in cyber incident response.
- Establish enhanced coordination procedures to prepare for significant cyber incidents that exceed its standing capacity, consisting of:
    - Dedicated leadership,
    - Supporting personnel,
    - Available facilities (physical and communications),
    - Internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.
- Identify the appropriate pathways for communicating with other state, local, and federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the State Homeland Security Advisor that enhanced coordination procedures were activated or initiated.
- Highlight internal communications and decision-making processes that are consistent with effective incident coordination.
- Outline processes for maintaining these procedures.
- In addition, OHS' enhanced coordination procedures will identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41.
- Maintain capacity and capability to obtain and maintain clearances and accesses to facilitate the quick sharing of information.
- Develop/update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident.
- Serve as state coordination point for cognizant federal entities.
- Advise the Governor on the need to declare a state emergency or request federal assistance.

4.1.1.1.1 THROUGH THE HSFC:

- Collect, analyze, and disseminate intelligence information.
- Conduct threat and risk analyses.
- Assist law enforcement as appropriate.
- Maintain liaison with the State EOC upon activation.

4.1.1.2 NATIONAL GUARD

The Hawai‘i National Guard (HING) is comprised of the Hawai‘i Army National Guard (HIARNG) and Hawai‘i Air National Guard (HIANG), with personnel across the State.

Hawai‘i Army National Guard - The HIARNG has a Defensive Cyber Operations Element (DCO-E) that may be deployable for state cyber disruption response. The DCO-E is primarily responsible for cybersecurity, information assurance and internal defense measures on the Department of Defense Information Network- National Guard (DoDIN-A NG) in a Title 32 U.S. Code (Title 32) status. Upon request for support, and with the approval of the Governor and Adjutant General, the HING DCO-E may also provide support for non-DoD mission partners in a State Active Duty (SAD) status. In certain circumstances, the DCO-E may be activated under Title 10 U.S. Code (Active Duty) status to meet immediate incident response needs.

Hawai‘i Air National Guard - The HIANG has several cyber Mission Defense Teams (MDTs) whose primary purpose is cyber defense of tasked DoD mission systems in Title 32 status. Upon request for support, and with the approval of the Governor and Adjutant General, HING MDT personnel may also provide support for non-DoD mission partners in a SAD status.

The HING also maintains units tasked with traditional information technology support who may also be available to support vulnerability assessment and cyber disruption recover efforts when in SAD status.

4.1.1.2.1 CAPABILITIES

Between the DCO-E and MDT, the HING may possess the capability to perform:

- Network security and vulnerability assessments
- Network Analysis
- Host-based Analysis
- Assessment and Detection
- Containment, Eradication, and Recovery support
- Collection and analysis of intrusion artifacts to enable mitigation efforts
- Cyber incident triage
- Threat data correlation to provide increased situational awareness

4.1.1.2.2 RESPONSE & RESPONSIBILITIES

All requests for HING support are thru State Emergency Support Function (SESF) Annex #20- Military Support, State of Hawai‘i Emergency Operations Plan (HI-EOP). In addition to responsibilities outlined in the HI-EOP, in a significant cyber incident (disruption) the HING:

- May assist in the analysis of incident information, development of situational awareness, and technical assistance to prevent, protect, respond to, recover from, and mitigate the effects of a cyber incident.
- May activate for external response assets upon request and gubernatorial approval.
- May provide cyber incident response, as directed by the governor and Adjutant General, regardless of scope or customer type.

- May provide initial outreach, liaison duties, or on-site assistance to critical infrastructure providers.
- May provide supplemental incident response personnel to help manage the incident and relieve personnel/reduce staff fatigue.
- May support State of Hawai'i Office of Homeland Security in the cyber threat information sharing mission.

4.1.1.2.3 AUTHORITIES AND AGREEMENTS

In December 2019, the Hawai'i Office of Enterprise Technology Services (ETS) signed a Memorandum of Understanding with the Hawai'i National Guard.

The Parties agreed "to collaborate to increase their capacity and capability to defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of the State of Hawai'i and the United States. The Parties agree to jointly conduct training exercises, cybersecurity threat and defense assessments, computer network defense operations, and incident response activities to protect the public health, welfare, and safety of Hawaii's citizens."

4.1.1.2.4 LIMITATIONS

HING members are not authorized to conduct intelligence activities, including foreign intelligence and counterintelligence, while operating under Title 32 or State Active Duty. HING personnel in State Active Duty are prohibited from accessing their federal security clearances without a federal sponsor. In consultation with HING legal representatives, the HING may be authorized to conduct shared situational awareness and information sharing activities in supporting of a state cyber disruption response.

4.1.1.3 EMERGENCY MANAGEMENT AGENCY

The Hawai`i Emergency Management Agency (HI-EMA) is established as the state emergency management agency by HRS 127A-3(a). HI-EMA maintains a comprehensive, coordinated, and cooperative emergency management program for the State, coordinating its activities with county emergency management agencies, federal agencies involved in emergency management, state departments and agencies, other states, the private sector, and non-governmental organizations (NGOs).

During a Cyber Disruption:

- Provide overall coordination for the state's response and recovery activities to any consequence management activities for physical effects related to the significant cyber incident, including activating the SEOC and SERT, provisioning resources requested by affected counties and state agencies and, when applicable, utilizing federal support. As appropriate, HIEMA's operation coordination will conform to the existing EOP processes.
- Advise the Governor on the need to declare a state emergency or request federal aid.

- At the direction of the Governor's office and in coordination with the Department of Attorney General, prepare state disaster proclamations and Presidential disaster requests for the Governor's signature.
- Coordinate requests for out-of-state mutual aid through the Emergency Management Assistance Compact (EMAC).

4.1.2 ATTORNEY GENERAL'S OFFICE

- Coordinate with appropriate prosecuting authorities for the prosecution of criminal cases brought by the state.

4.2 AFFECTED ENTITY(IES)

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber incidents that damage computer systems can cause lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by all levels of governments, businesses, consumers, and all other users of the Internet. An entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents.

When supporting affected entities, the various agencies of the Federal, State, and Local Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities to minimize impacts to assets/systems, reduce their vulnerabilities, and bring malicious actors to justice.

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the State and Federal Government. Accordingly, all victims are encouraged to report all cyber incidents as detailed in Section 3.2.2 Notification and Activation.

4.3 FEDERAL GOVERNMENT LINES OF EFFORT

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: **Threat Response** and **Asset Response**. Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.[34]

The 2016 Presidential Policy Directive (PPD) 41, United States Cyber Incident Coordination articulates the principles governing the U.S. Federal Government's response to any cyber incident and, for

[34] U.S. Department of Homeland Security. (Undated). *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. Accessed October 28, 2021 at: https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

significant cyber incidents, establishes lead federal agencies and an architecture for coordinating the broader Federal Government response. The Federal Government has three lines of effort in cyber incident response. No single agency possesses all the authorities, capabilities, and expertise to deal unilaterally with a significant cyber incident.

Asset response efforts involve furnishing technical assistance to affected entities to help them recover from the incident. The Department of Homeland Security (DHS), through the National Cybersecurity and Communications Integration Center (NCCIC), is the lead federal agency for asset response activities for significant cyber incidents. Such activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.[35]

Threat response efforts involve the investigation of the crime. The Department of Justice (DOJ), through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), is the lead federal agency for threat response activities for significant cyber incidents. Such activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.[36]

Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available Federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned during the response; and facilitating information sharing and operational coordination with other Federal Government entities.[37]

Intelligence support and related activities are coordinated by the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, as the Federal lead agency for intelligence support and related activities. Such activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.[38]

[35] The White House. (2016, July). *Presidential Policy Directive – United States Cyber Incident Coordination.* Accessed September 13, 2021 at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[36] Ibid.
[37] Ibid.
[38] Ibid.

5. DIRECTION, CONTROL, AND COORDINATION

Any agency receiving initial reporting of a significant cyber incident will coordinate with all other relevant state, local, and federal stakeholders in responding to the incident, including determining whether to establish a Cyber Unified Coordination Group (UCG) to coordinate the response to the significant cyber incident.

5.1.1 State Cyber Unified Coordination Group

Formation. A Cyber Unified Coordination Group (C-UCG) will be formed and activated only in the event of a significant cyber incident and will be incident specific. A C-UCG may be formed by any of the following processes:

- At the direction of the Governor or the State Homeland Security Advisor;
- When two or more state or state and local agencies request its formation based on their assessment of the cyber incident against the severity schema; and or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Office of Homeland Security for which a cyber incident could reasonably result in catastrophic state, regional, or national effects on public health or safety, economic security, or national security.

Dissolution. A C-UCG will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one state/local agency are no longer required to manage the remaining facets of the state response to an incident.

Responsibilities. To promote unity of effort in response to a significant cyber incident, a C-UCG will:

- Coordinate the cyber incident response in a manner consistent with the principles described in PPD-41;
- Ensure all appropriate State, local, and Federal agencies are incorporated into the incident response;
- Coordinate the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
- Facilitate the rapid and appropriate sharing of information and intelligence among C-UCG participants on the incident response and recovery activities;
- Coordinate consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders, including the public as appropriate; and

- For incidents that include cyber and physical effects, form a combined UCG with the lead State, local, and Federal agencies or with any UCG established to manage the physical effects of the incident under the National Response Framework developed pursuant to PPD-8 on National Preparedness.

A C-UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive private sector information.

The C-UCG will promptly coordinate with the State Attorney General, county Corporation Counsel, DOJ, general counsel from DHS, regulators, and other relevant state and federal agencies' attorneys about pertinent legal issues as they are identified to quickly consider and coordinate them with appropriate nongovernmental entities, as necessary.

Participation. In response to a significant cyber incident that includes the need to engage in consequence management activities for physical effects related to the incident, the State Government establishes two lead agencies:

- OHS is the lead agency for coordinating asset and threat response and intelligence support during a significant cyber incident.
- HI-EMA is the lead agency for coordinating response to any consequence management activities for physical effects related to the significant cyber incident.

OHS will administer and manage the state's incident handling efforts and coordinate as appropriate with whole community partners.

Upon implementation of the ***HI-EOP*** and activation of the State EOC, the Director of Emergency Management or designee will establish operational command, coordination of state resources and support organizations required for consequence management in accordance with the ***HI-EOP***.

The HI-EMA will manage and utilize the State EOC and coordinate with OHS to receive and disseminate information and intelligence, establish common strategic priorities and operating picture, and prioritize short-, intermediate- and long-term activities among the relevant organizations.

When a Cyber UCG is established, in addition to the two state lead agencies, OHS and HI-EMA, the Cyber UCG will also include relevant state and/or local coordinating agencies if the cyber incident affects or is likely to affect sectors they have coordinating authority/responsibility for, as well as other state/local cybersecurity centers, as deemed necessary per the specific significant cyber incident.

Like government participation, private sector involvement in a C-UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response. Private Sector Cyber UCG participation will be voluntary, and participants should be from organizations which can determine the incident priorities for each operational period and approve an Incident Action

Plan, to include commitment of their organizations' resources to support execution of the Incident Action Plan. Per the Guiding Principles in PPD-41, out of respect for an affected entities' privacy and sensitive private sector information, the State Government will coordinate with the affected entity on the approach of wider incident dissemination for that incident. C-UCG participants will be expanded or contracted as the situation changes during that incident response.

Regardless of specific participant composition, a C-UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive and protected private sector information.

6. PLAN DEVELOPMENT AND MAINTENANCE

This ***CDRP*** is developed with input from federal, state, non-governmental and private sector entities that will support a state IT enterprise cyber incident.

The OHS is responsible for coordinating all revisions to this Plan. Maintenance responsibilities include:

- Maintaining a plan review schedule.
- Reviewing all plan components and proposed changes for consistency.
- Obtaining approvals for changes from the appropriate approving authority.
- Ensuring notifications of approved changes are made and maintaining a record of changes.
- Coordinating changes through with ETS to synchronize with the ***CIRP*** and to ensure consistency with the ***HI-EOP***.

Review Cycle. OHS will complete periodic updates of this plan no less than every two years. Updates may be initiated to address any of the following:

- Minor administrative revisions needed to update terminology, titles, or agency names.
- Ensure risk and vulnerability analysis, planning assumptions and situation reflect current realities.
- Address relevant changes in federal or state laws, policies, structures, capabilities or other changes to emergency management standards or best practices.
- Incorporate substantive lessons learned from exercises, incident analysis or program evaluations.

7. AUTHORITIES AND REFERENCES

7.1 STATE LAWS, REGULATIONS AND DIRECTIVES

1. ***Hawai'i Revised Statutes (HRS) Chapter 128A.*** Homeland Security.
2. ***Hawai'i Revised Statutes (HRS) Chapter 128B.*** Cybersecurity.
3. ***Hawai'i Revised Statutes (HRS) Chapter 487N.*** Security Breach of Personal Information.
4. ***Hawai'i Revised Statutes (HRS) Chapter 127A.*** Emergency Management.

7.2 FEDERAL LAWS, REGULATIONS AND DIRECTIVES

1. ***Cybersecurity and Infrastructure Security Agency Act of 2018.*** Elevated the mission of the former National Protection and Programs Directorate within DHS and established the Cybersecurity and Infrastructure Security Agency (CISA).
2. ***U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan, January 2017.*** In response to increased concern about the potential impacts to the electric grid from an electromagnetic pulse (EMP) the U.S. Department of Energy developed an EMP resilience strategy in coordination with the electric power industry. This Action Plan is structured to address each of the five strategic goals defined in that Joint Strategy and describes a series of actions for each goal.
3. ***National Cyber Incident Response Plan, December 2016.*** Recognized that the frequency of cyber incidents is increasing, and the trend is unlikely to be reversed anytime soon. It also acknowledged that the most significant of these incidents necessitate deliberative planning, coordination, and exercising of response activities.
4. ***Cybersecurity Act of 2015.*** Legislation that allows companies in the U.S. to share personal information related to cybersecurity with the government. The government could use this information as evidence to prosecute crimes.
5. ***Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 2013.*** This directive establishes national policy on critical infrastructure security and resilience. This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration.
6. ***National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, 2013.*** This plan describes a national unity of effort to achieve critical infrastructure security and resilience. Based on the guidance in the National Plan, the partnership will establish and pursue a set of mutual goals and national priorities and employ common structures and mechanisms that facilitate information sharing and collaborative problem solving.
7. ***Health Insurance Portability and Accountability Act (HIPAA) of 1996.*** Under HIPAA, protected health information is individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses).

8. ***Gramm-Leach-Bliley Act (GLBA) of 1999.*** The GLBA requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

7.3 REFERENCES

1. *State of Hawai'i Cyber Incident Response Plan (CIRP), March 2022.*
2. *Cybersecurity Incident & Vulnerability Response Playbooks,* November 2021
3. *FBI Releases IC3 2019 Internet Crime Report,* February 2020.
4. BlueVoyant - *State and Local Government Security Report,* August 2020.
5. Booz-Allen-Hamilton - *2021 Cyber Threat Trends Outlook,* 2020.
6. DARKReading - *Local, State Governments Face Cybersecurity Crisis,* June 2020.
7. GCN - *Cyberattacks on state, local government up 50%,* September 2020.
8. *Worldwide Threat Assessment of the US Intelligence Community,* January 2019.
9. *National Cyber Awareness System*, November 2019.
10. *State of Hawai'i Emergency Operations Plan (EOP),* November 2019.
11. Security.org - *What States Are at Highest Risk for Cyberattacks,* August 2019.
12. National Governor's Association - *Issue Brief: State Cyber Disruption Response Plans,* July 2019.
13. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security,* October 2016.
14. *Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology,* August 2012.
15. *NASA-Funded Study Reveals Hazards of Severe Space Weather,* January 2009.
16. CrowdStrike Services - *You've Been Breached – Now What?: How to Respond to a Worst-Case Cyber Scenario,* undated.
17. Check Point Software Technologies LTD - *What Is A Cyber Attack?,* undated.

8. ATTACHMENTS

Attachment 1 – Acronyms
Attachment 2 – Checklist of Major Steps for Disruption Response and Handling
Attachment 3 – Model Cyber Incident Response Plan
Attachment 4 – Cyber Incident Severity Schema/National Response Coordination Center Activation Crosswalk
Attachment 5 – Core Capabilities and Critical Tasks
Attachment 6 – Guidance on Reporting a Cyber Disruption
Attachment 7 – Threat Levels and Anticipated Response
Attachment 8 – Communications Checklists

ABBREVIATIONS AND ACRONYMS

The following is a list of some of the common abbreviations and acronyms in this plan:

AI	Artificial Intelligence
C-UCG	Cyber Unified Command Group
CDRP	Cyber Disruption Response Plan
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
DCO-E	Defensive Cyber Operations Element
DHS	Department of Homeland Security
DNC	Democratic National Committee
DoD	Department of Defense
DoDIN-A NG	Department of Defense Information Network- National Guard
DOJ	Department of Justice
ECTF	Electronic Crimes Task Force
EMP	Electromagnetic Pulse
EOC	Emergency Operations Center
ETS	Office of Enterprise Technology Services
FBI	Federal Bureau of Investigation
GLBA	Gramm-Leach-Bliley Act
HI-EOP	Hawai‘i Emergency Operations Plan
HIANG	Hawai‘i Air National Guard
HIARNG	Hawai‘i Army National Guard
HING	Hawai‘i National Guard
HIPAA	Health Insurance Portability and Accountability Act
HRS	Hawai‘i Revised Statutes
HSFC	Hawai‘i State Fusion Center
HSI	Homeland Security Investigations
ICE	Immigration and Customs Enforcement
IOT	Internet of Things
IT	Information Technology
MDT	Mission Defense Team
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
OHS	Office of Homeland Security
PPD	Presidential Policy Directive
SAD	State Active Duty

SESF	State Emergency Support Function
SOP	Standard Operating Procedure
USCG	United States Coast Guard
USINDOPACOM	United States Indo-Pacific Command

CHECKLIST OF MAJOR STEPS FOR SIGNIFICANT INCIDENT RESPONSE AND HANDLING

	Action	Completed
	Detection and Analysis	
1.	Determine whether and incident has occurred.	
1.1	Analyze the precursors and indicators.	
1.2	Look for correlating information.	
1.3	Perform research (e.g., search engines, knowledge base).	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Prioritize handling of the incident based on the relevant factors (e.g., functional impact, information impact, recoverability effort, etc.).	
3.	Report the incident to the appropriate internal personnel and external organizations.	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence.	
5.	Contain the incident.	
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	
6.2	Remove malware, inappropriate materials, and other components.	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.	
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	
7.2	Confirm that affected systems are functioning normally.	
7.3	If necessary, implement additional monitoring to look for future related activity.	
	Post-Incident Activity	
8.	Create a follow-up report.	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise).	

Source: NIST Special Publication 800-61, revision 2

MODEL CYBER INCIDENT RESPONSE PLAN

Public and private sector entities should consider creating an entity-specific operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Each organization should consider a plan that meets its unique requirements and relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2)[1] outlines several elements to consider when developing a cyber incident response plan. Each plan should be tailored and prioritized to meet the needs of the organization and adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. As appropriate, public, and private sector entities are encouraged to collaborate in the development of cyber incident response plans to promote shared situational awareness, information sharing, and acknowledge sector, technical, and geographical interdependences.

The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan:[2]

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk assessments
- Cyber Incident Scoring System/Criteria[3]
- Incident reporting and handling requirements
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization
- Communications with outside parties, such as:
    - Customers, constituents, and media
    - Software and support vendors
    - Law enforcement agencies
    - Incident responders

[1] National Institute of Standards and Technology. (2012, August). SP 800-61: Computer Incident Handling Guide, Revision 2. Accessed November 3, 2021 at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[2] U.S. Department of Homeland Security. (2016, December). *National Cyber Incident Response Plan, Annex C*. Accessed September 10, 2021 at: National Cyber Incident Response Plan - December 2016 (cisa.gov)

[3] The National Cybersecurity and Communications Integration Center Cyber Incident Scoring System could be used as a basis for an organizations operations center to assist in the internal elevation of a particular incident. https://www.us-cert.gov/NCCIC-Cyber-Incident-ScoringSystem.

  - Internet service providers
  - Critical infrastructure sector partners
- Roles and responsibilities (preparation, response, recovery)
  - State Fusion Center
  - Emergency Operations Center
  - Local, regional, state, tribal, and territorial government
  - Private sector
  - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process.

CYBER INCIDENT SEVERITY SCHEMA / NATIONAL RESPONSE COORDINATION CENTER ACTIVATION CROSSWALK

When incidents impact the cyber and/or physical environment(s), certain decisions and activities require coordination in order to respond in the most appropriate manner. The graphic below compares the Cyber Incident Severity Schema released in Presidential Policy Directive 41: United States Cyber Incident Coordination and the Department of Homeland Security National Response Coordination Center Activation Scale when comparing response levels for cyber and physical incidents.

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

CORE CAPABILITIES AND CRITICAL TASKS

Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

1. Access Control and Identity Verification Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization.
Critical Tasks: • Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. • Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performing as intended. • Conduct training to ensure staff-wide adherence to access control authorizations.
2. Cybersecurity Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.
Critical Tasks: • Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. • Secure, to the extent possible, public, and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. • Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
3. Forensics and Attribution Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.
Critical Tasks: • Retrieve digital media and data network security and activity logs. • Conduct digital evidence analysis, and respecting chain of custody rules. • Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary. • Assess capabilities of likely threat actors(s). • Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s). • Interview witnesses, potential associates, and/or perpetrators if possible.

• Apply confidence levels to attribution assignments. • Include suitable inclusion and limitation information for sharing products in attribution elements guidance. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performed as intended.
4. Infrastructure Systems Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.
Critical Tasks: • Maintain a comprehensive understanding of the needs for the safe operation of control systems. • Stabilize and regain control of infrastructure. • Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities. • Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident. • Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.
5. Intelligence and Information Sharing Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.
Critical Tasks: • Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats. • Share analysis results through participation in the routine exchange of security information— including threat assessments, alerts, threat indications and warnings, and advisories—among partners. • Confirm intelligence and information sharing requirements for cybersecurity stakeholders. • Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.42 • Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts. • Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness. • Enable collaboration via online networks that are accessible to all participants. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
6. Interdiction and Disruption Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.
Critical Tasks: • Deter malicious cyber activity within the United States, its territories, and abroad. • Interdict persons associated with a potential cyber threat or act.

• Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s). • Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation's public and private information systems. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
7. Logistics and Supply Chain Management Description: Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Critical Tasks: • Identify and catalog resources needed for response, prior to mobilization. • Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident. • Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems. • Enhance public and private resource and services support for impacted critical infrastructure entities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Apply supply chain assurance principles and knowledge within all critical tasks identified above.
8. Operational Communications Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.
Critical Tasks: • Ensure the capacity to communicate with both the cyber incident response community and the affected entity. • Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders. • Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail. • Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. • Protect individual privacy, civil rights, and civil liberties. • Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).43 • Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility
9. Operational Coordination Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.
Critical Tasks:

• Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident. • Define and communicate clear roles and responsibilities relative to courses of action. • Prioritize and synchronize actions to ensure unity of effort. • Ensure clear lines and modes of communication between entities, both horizontally and vertically. • Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.
10. Planning Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.
Critical Tasks: • Initiate a flexible planning process that builds on existing plans as part of the National Planning System.44 • Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities. • Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors. • Inform risk management response priorities with critical infrastructure interdependency analysis. • Identify and prioritize critical infrastructure and determine risk management priorities. • Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and federal organizations and agencies. • Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources. • Formalize partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner. • Formalize partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalize relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary. • Formalize partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
11. Public Information and Warning Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding

significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.
Critical Tasks: • Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public. • Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government. • Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect applicable information sharing and privacy protections, including Traffic Light Protocol. • Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.
12. Screening, Search, and Detection Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.
Critical Tasks: • Locate persons and networks associated with cyber threats. • Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners). • Conduct physical and electronic searches as authorized by law • Collect and analyze information provided. • Detect and analyze malicious cyber activity and support mitigation activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.
13. Situational Assessment Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.
Critical Tasks: • Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions. • Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements. • Develop a common operational picture for relevant incident information shared by more than one organization. • Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
14. Threats and Hazards Identification Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.
Critical Tasks: • Identify data requirements across stakeholders.

- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate, and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

GUIDANCE ON REPORTING A CYBER DISRUPTION

ESCALATION

A cyber disruption should be reported if it was determined that the affected entity has experienced the following impact upon detection:

Functional Impact	• Incidents impacting the business functionality of critical IT systems resulting in some type of negative impact to the users, business processes, etc. (e.g. DDoS, Ransomware, etc.)
Information Impact	• Incidents that affect the confidentiality, integrity, and availability of the entity's information resources (e.g. DDoS, Ransomware, etc.)
Recoverability Efforts	• It is not possible to recover from an incident due to unforeseen circumstance as it would require addition resources on the incident handling cycle; unless that effort was directed at ensuring that a similar incident did not occur in the future.

COMMUNICATION

The reporting entity should maintain records about the status of incidents, along with other pertinent information. The incident report should contain information on the following:

- Brief description of the incident and what was impacted
- Contact information for all parties involved
- Status of the incident (If possible, other incidents related to this incident)
- Indicators related to the incident (e.g. malicious IP addresses, domains, hashes etc.)
- Actions taken by all incident handlers on this incident (e.g. chain of custody and comments from incident handlers, etc.)
- A list of evidence gathered during the incident investigation (e.g. forensic acquisitions, network logs, etc.)

THREAT LEVELS AND ANTICIPATED RESPONSE

Threat Level	Description	Potential Impact	Communication Activity	Anticipated Response Activity
Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services	Widespread outages, and/or destructive compromise to systems with no known remedy, or one or more critical infrastructure sectors debilitated	State EOC coordinates all communications CSTF activities	State EOC, Governor's Unified Command activated and is represented at State EOC
Severe	Likely to results in a significant impact to public health and/or safety	Core infrastructure targeted or compromised causing multiple outages, multiple system compromises or critical infrastructure compromises	- Notify and convene by phone or in person - DAGS/ETS to activate CSTF and report incident to MS-ISAC, HSFC & HI-EMA	- Voluntary resource collaboration among CSTF members - Info sharing - Communications/messaging - Possible State EOC Activation
High	Likely to result in a discernable impact to public health, safety or confidence	Compromised systems or diminished services	- Notify DAGS/ETS - ETS-CST to report incident to MS-ISAC - CSTF may be activated at this level	Real-time collaboration via phone and email as required. Activity can be conducted remotely.
Medium	May affect public health, safety, and/or confidence	Potential for malicious cyber activities, no known exploits, or known exploits, identified but no significant impact has occurred.	- Contact DAGS/ETS and share with affected department/agencies and any that may be affected. - ETS-CST to report incident to MS-ISAC	Informational only. No follow-up activity required. No real-time collaboration.
Low	Unlikely to affect public health, safety, and/or confidence	Normal concern for known hacking activities, known viruses, or other malicious activity	- Contact DAGS/ETS if discovered by another State dept/agency	None expected

Table 1 State of Hawai'i Cyber Security Response Matrix

The table above provides the Cyber Security Threat Levels identified for the State of Hawaii, with potential impacts and general anticipated response activity.

The State of Hawaii Cyber Security Response Matrix consists of 5 distinct levels, which are affected by internal and/or external cyber security events. The matrix provides general guidance of the communication and anticipated responses activities for each threat level. This section provides the following information for each threat level:

- Level definition – a brief description of what each security level means;
- Escalation/De-escalation criteria – description of the variables that are in place for alert level to change;
- Potential impact – how the level affects state agencies, municipalities, and the public;
- Communications procedures – how the knowledgeable party communicates with the ETS-CST, CSTF, the HSFC, or other response partners in order to inform affected individuals and organizations of the threat;

It is important to note that these threat levels are based on the risk an event poses and the impact it has, particularly on the state government enterprise. Incidents may require the ETS-CST and/or CSTF to skip levels, and/or to address an intervening threat before returning to the originating level after that threat has been mitigated.

1. CYBER SECURITY THREAT LEVEL – EMERGENCY

At Level EMERGENCY, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical state government information technology infrastructure and assets. These attacks have an impact at the national, state, and local levels.

If a Cyber Security Threat Level EMERGENCY occurs within the state information technology enterprise _____ must be notified of the incident as soon as possible. _____ will be informed as part of the response process.

- Definition: Malicious activity has been identified with a catastrophic level of damage or Incident. Examples include but are not limited to:
  - Malicious activity results in widespread outages and/or complete network failures;
  - Data exposure with severe impact;

  - Significantly destructive compromises to systems, or disruptive activity with no known remedy;
  - Mission critical application failures with imminent or demonstrated impact on the health, safety, or economic security of the state;
  - Compromise or loss of administrative controls of critical system;
  - Loss of critical Land Mobile Radio and other critical State infrastructure.
- Actions:
  - Continue recommended actions from previous levels; Data exposure with severe impact;
  - Shut down connections to the Internet and external business partners until appropriate corrective actions are taken;
  - Ensure that potential threats are disseminated and outreach for prevention purposes is made to other entities;
  - Contact appropriate law enforcement partners to pursue enforcement actions through investigation and criminal prosecution;
  - Isolate internal networks to contain or limit the damage or Incident.
  - Governor to initiate Robert T. Stafford Relief and Emergency Assistance Act
- Escalation: To raise the threat level to Level EMERGENCY, the following conditions must be in place: The threat has affected multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.
- Potential Impact:
  - Impact to IT Services:
    - Telecommunications are unavailable making it necessary to use alternate forms of communication;
    - The power grid is unreliable causing agencies to rely on backup generators or uninterrupted power supply (UPS);
    - Buildings have been damaged or destroyed rendering IT resources inoperable;
    - Relocation to State EOC for command and control purposes; Agency(ies) Incident/Incident Response Plan(s) activated;
    - Response activities must be implemented to restore IT operations and/or to address damages from the cyber-attack;
    - Data centers have to be restored or relocated to alternate facilities;
    - The issues raised by the Incident will take over six business days to remediate and critical applications and services will be offline until the issues are resolved;
    - The threat can only be remediated by restoring the applications systems, and facilities to an operational state by rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.
  - Agency Impact:
    - Agency IT staff will work to restore equipment, systems, and applications to an operational state;

  - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues, which may arise from the Incident.
- Communications Procedures: At Level EMERGENCY, he state/municipal critical IT resources are rendered inoperable by a cyber security attack that will take weeks to recover. Such an event will affect IT communications and necessitate the need for alternate forms of communication (e.g., satellite, radios, messengers).
  - State EOC – The State EOC will be activated, and the following State EOP, the Governor's Unified Command will meet there.
  - Work with the State EOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
  - CIO will ensure that MS-ISAC is notified, and request assistance if necessary.
  - Pursuant to the State EOP, a WebEOC incident may be opened and WebEOC used to provide situational awareness, process requests for assistance, etc.
  - Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
  - Messengers-Depending on the nature of the event, the state may use messengers to communicate information between incident responders and the State EOC.
- De-Escalation Criteria: To return to Level SEVERE or below, the Incident must pass the escalation criteria identified within each section.

2. CYBER SECURITY THREAT LEVEL – SEVERE

Level SEVERE signifies confirmed cyber-attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised (state/municipal) IT resources and are using them to propagate the attack or to spread misinformation.

If a Cyber Security Threat Level SECURE occurs within the state information technology enterprise, _____ , and _____ must be notified of the incident as soon as possible. The Hawaii State Fusion Center shall be informed as part of the response process.

- Definition: Malicious activity has been identified in (state/municipal) networks with a major level of damage or Incident. Examples include but are not limited to:
  - Malicious activity affecting core infrastructure;
  - A vulnerability is being exploited and there has been major impact;
  - Data exposed with major impact;
  - Multiple system compromises or compromises of critical infrastructure;
  - Attackers have gained administrative privileges on compromised systems in multiple locations;

- Multiple damaging or disruptive malware infections;
- Mission critical application failures but no imminent impact on the health, safety, or economic security of the state;
- A distributed denial of service attack with major impact.

- Actions:
  - Refer to Matrix in Table 1 for communications flow;
  - Continue recommended actions from previous levels;
  - Agency(ies) Incident/Incident Response Plan(s) activated;
  - Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, and system log files for unusual activity;
  - Consider limiting or shutting down less critical connections to external networks such as the internet;
  - Consider isolating less mission critical internal networks to contain or limit the potential of an incident;
  - Fax, phone (where available) or state radio network in lieu of email and other forms of electronic communication;
  - When available, test and implement patches, anti-virus updates, and other measures immediately;
  - State EOC activation based on conditions, following the State EOP. Voluntary resource collaboration, technical information sharing and resource deployment, including mutual aid if needed. May include financial considerations.
  - Governor to consider initiating Robert T. Stafford Relief and Emergency Assistance Act if deemed necessary.
- Potential Impact:
  - Impact to IT Services could include:
    - A critical vulnerability is being exploited and there has been a significant impact;
    - Telecommunications may be interrupted causing agencies to use alternate forms of communication;
    - Email communications may be disrupted or untrusted, making it necessary for agencies affected by the event to use alternate forms of communications;
    - Relocation to the State EOC for command and control purposes;
    - Agency IT Operations may have to be relocated to the State EOC for command and control purposes;
    - Response activities may have to be implemented to restore IT operations and/or to address damages from the cyber-attack;
    - Normal grid supplied power may become unreliable/unavailable for extended periods of time and considerations of emergency backup power are being prioritized;
    - Multiple damaging or disruptive virus attacks; and/or multiple denial of service attacks against critical infrastructure services;

        - The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems or applications to a previous date before the attacks occurred;
    - Agency Impact:
        - Agency IT staff will work with ETS to restore equipment, systems, and applications to an operational state;
        - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues that may arise from the Incident.
    - Municipal Sector:
        - Impacts to municipal infrastructure and operations will be monitored following the State EOP, and requests for mutual aid will be received for consideration at the State EOC, including assistance to contain or address the cyber incident.
- Communication Procedures: At Level SEVERE, the (state/municipal) IT critical resources have been severely affected by a cyber security event that has caused IT service to be offline/unreliable for an extended period. This event may affect telecommunications and may cause incident responders to use alternate forms of communication.
    - The responding personnel will be notified via email if available, cell phone or messenger, will activate the Incident Response Plan, and will recommend a State EOC activation.
    - The responding personnel will work with the State EOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
    - Senior responding personnel or CIO will ensure that MS-ISAC is notified, and request assistance if necessary.
    - Email will be used if available to communicate alerts, status reports, updates, and ancillary information.
    - Pursuant to the State EOP, a WebEOC incident may be opened and WebEOC used to provide situational awareness, process requests for assistance, etc.
    - Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
    - Messengers – Depending on the nature of the event, the state may use messengers to communicate information among incident responders, the responding personnel, and the State EOC.
- De-Escalation Criteria: To return to Level HIGH or below, the incident must pass the escalation criteria identified within that section.

3. CYBER SECURITY THREAT LEVEL – HIGH

If a Cyber Security Threat Level HIGH occurs within the state information technology enterprise, _____ , _____ and, _____ shall be notified of the incident.

- Definition: Malicious activity has been identified in (state/municipal) networks with a moderate level of damage or Incident.
- Examples include but are not limited to:
  - An exploit for a vulnerability that has a moderate level of damage;
  - Compromise of secure or critical system(s);
  - Compromise of systems containing sensitive information or non-sensitive information;
  - More than one agency affected in the (state/municipal) network with moderate level of impact;
  - Infected by malware spreading quickly throughout the Internet with moderate impact;
  - A distributed denial of service attack with minor impact.
- Actions:
  - Refer to Matrix in Table 1 for communications flow;
  - Continue recommended actions from previous levels;
  - Agency(ies) Incident/Incident Response Plan(s) activated identify vulnerable systems;
  - Increase monitoring of critical systems;
  - Contact senior responding personnel for additional guidance;
  - Immediately implement appropriate counter-measures to protect vulnerable critical systems;
  - When available, test and implement patches, install anti-virus updates, and other system security measures as soon as possible;
  - Contact DAGS/ETS. HSFC and HI-EMA will be contacted for situational awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes;
  - Real time collaboration via phone and email as required;
  - Consider State EOC activation;
  - Governor to consider initiating Robert T. Stafford Relief and Emergency Assistance Act if deemed necessary.
- Escalation Criteria: In order to raise the state/municipal agency threat level to Level HIGH, the threat must involve two or more agencies or critical infrastructure sectors, critical applications, or websites; and/or the risk of the threat has been determined to have a significant impact to (state/municipal) IT operations.
- Potential Impact: At Level HIGH, the following conditions are in place:
  - Impact to IT Services could include:

- There are multiple web defacements;
- A critical vulnerability is being exploited and there has been moderate impact;
- Attackers have gained administrative privileges on compromised systems;
- Critical applications or resources have been affected;
- Compromise of secure or critical system(s) containing sensitive information;
- Compromise of critical system(s) containing non-sensitive information, if appropriate;
- IT services may be interrupted by denial of service attacks;
- The issue can be remediated within one to three business days and may require that critical application or services be taken offline until the issue can be remediated;

  - Continuity of Operations Plan(s)/Continuity of Government Plans(s) (COOP)/COG) may have to be initiated to address the damages from the cyber-attack.
  - Remediation Effort: The threat can be remediated by (state/municipal) agencies installing software patches, updating anti-virus files, or denying network access to specific Ips or IP ranges.
  - Agency Impact:
    - Agency IT staff will work DAGS/ETS CSTF and with Subject Matter Experts (SMEs) from various agencies to install software patches, update anti-virus files, or deny network access to specific Ips or IP ranges;
    - Agency(ies) Incident/Incident Response Plan(s) activated;
    - If state is affected responding personnel will work with the Governor's Office /Unified Command and the Attorney General to address any ramifications, including political or legal issues that may arise from the incident;
  - Responding personnel will work with State EOC, if activated, to address any communication or facility needs required by the agency to address the Incident.

- Communication Procedures: At Level HIGH situation means that some of the (state/municipal) IT critical resources have been affected by a cyber security event or that multiple agencies have had significant security breaches. At this level, the following communications methods may be utilized:
  - Refer to Matrix in Table 1 for communications flow, which includes:
    - The CSTF will be convened by the State CIO via email, telephone, cell phone or messenger and the Team will start making preparations to enact the State Cyber Incident Response Plan and this CIRP.
    - Senior responding personnel or CIO will ensure that responding personnel are notified. Responding personnel may also request assistance with remediating the issue;
    - Responding personnel, through HSFC or other means, will notify designated individuals/groups and provide it with updates or remediation information;

  - Email will be used to communicate alerts, status reports, updates and ancillary information. In case none of previously listed methods are available, mobile devices and LMR will be used as a means of communicating;
  - Telecommunications such as landlines and cell phones will be used for clarification purposes and to address questions about remediations efforts. In case none of previously listed methods are available, LMR will be used as a means of communicating;
- De-Escalation Criteria: To return to Level MEDIUM or below, the incident must pass the criteria defined within that section.

4. CYBER SECURITY THREAT LEVEL – MEDIUM

If a Cyber Security Threat Level MEDIUM occurs within the state information technology enterprise and can be handled without serious effects within the enterprise and without any external effects. The affected entity should notify ETS-CST for intelligence collection purposes, including monitoring trends.

- Definition: This is the first active threat level in the cyber security response matrix. Level MEDIUM means that malicious activity has been identified on state, municipal networks with minor impact.
- Examples include but are not limited to:
  - Change in normal activity with minor impact IT operations;
  - A critical vulnerability, with the potential to cause significant damage if exploited, has been detected;
  - A vulnerability is being exploited and there has been minor impact;
  - Infection by malware with potential to spread quickly;
  - Compromise of non-critical system(s) that did not result in loss of sensitive data;
  - A distributed denial of service attack with minor impact.
- Actions:
  - State agencies need to contact ETS-CST, which will interface with MS-ISAC for information sharing and additional guidance;
  - Continue recommended action from previous level;
  - Agency(ies) Incident/Incident Response Plan(s) activated;
  - Identify vulnerable systems and implement appropriate countermeasures;
  - Identify malware on system and remediate accordingly;
  - Document data exposure with minor impact;
  - When available, test and implement patches, install anti-virus updates, and other security measures in next regular cycle;

  - Contact only other agencies/departments if there is a potential to be affected as well.
- Escalation Criteria:
  - In order to raise the state agency threat level to Level MEDIUM, the State CIO or equivalent at government level must determine that the following conditions are in place: The threat is limited to one agency, application, or website; and/or the risk of threat is low and it can be easily remediated without having a long-term impact to state, municipal, or the State of Hawaii residents and/or visitors.
- Potential Impact: At Level MEDIUM, the following conditions are in place:
  - Impact to IT services:
    - There is no threat to mission critical applications or resources;
    - The issue has been properly identified and can easily be remediated without risk of a data breach or theft of services;
    - The issue can be remediated within normal business hours;
    - The threat can be easily remediated by State agencies following normal procedures (e.g. software patches, updating virus files).
  - Special Events/Circumstances: A special event or circumstance incites hackers interested in trying to disrupt an agency IT services or deface a website, etc.
  - Agency impact: IT staff will take proactive measures. Impact to IT services should be minimal sine the threat has been identified and countermeasures exist for remediation.
- Communication Procedures: All IT resources are still operational. Communications will proceed as usual, with notification to ETS-CST, affected department/agencies, MS-ISAC and other partners as appropriate. See Table 1 Matrix. Email will be used to provide any alerts, status reports, updates and ancillary information to critical infrastructure owners and operators. Landlines and cell phone will be used for any clarification purposes and to address questions about remediation efforts.
- De-Escalation Criteria: To return to Level – LOW, any issues must be completely resolved, and agencies must confirm that IT resources are working normally and/or the circumstance has passed.

5. CYBER SECURITY THREAT LEVEL – LOW

Agencies and organizations conduct the following activities on an ongoing basis:

If a Cyber Security Threat Level LOW occurs within the state information technology enterprise, and can be handled without negative impacts outside the enterprise, no need to inform CSTF for intelligence collection purposes, including monitoring trends.

- Definition: Insignificant or no malicious activity has been identified. Examples include but are not limited to:
  - Credible warnings of increased probes or scans in a State, municipal network;
  - Infection by known low risk malware;
  - Other like incidents;
  - Normal activity with low level of impact.
- Actions:
  - Continue routine preventative measures;
  - Continue routine security monitoring;
  - Determine baseline of activity for the State/municipality/business—it is important to know what "normal" looks like;
  - State agencies need to contact ETS-CST, which will interface with MS-ISAC for information sharing and additional guidance if needed;
  - Ensure all personnel receive proper training on cyber security policies and security best practices.
- Escalation criteria: Infrastructure is operating normally and there are no known major cyber threats at this time
- De-Escalation criteria: In order to return to this level, the conditions that caused the change must be remediated.
- Potential impact: No cyber-related issues should be affecting state IT resources.
- Communication procedures: Besides day-to-day operational communications, no special communication procedures are required.

COMMUNICATIONS CHECKLISTS

A cyber disruption has the potential to cast a negative light on the State of Hawai'i - as well as to undermine faith in the State and possibly the Federal Government. If you are uncertain whether a situation could escalate into a crisis, err on the side of standing up response teams, because you can always stand down if the incident does not escalate. The checklists below can be adapted to account for various circumstances.

Action: Before a cyber crisis

- ☐ Identify protocol and the memberships of the technical response team(s).
- ☐ Create a list of terms with common cyber incident nomenclature for use by all stakeholders.
- ☐ Set an internal communication plan with key staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for dissemination and interfacing with the public/media.)
- ☐ Ensure that all stakeholders can be reached in a crisis without access to the affected systems, network or enterprise, including smart phones.
- ☐ Where appropriate and possible, establish contact with all appropriate entities responsible for cybersecurity. Also, understand in advance the legal obligations regarding the personal and/or sensitive data held by the organization.
- ☐ Establish contact with technology providers about potential threats and ensure that they know the technical and policy support functions available to them.
- ☐ Conduct briefings for members of the media.
- ☐ Get your social media account verified, because it will provide priority access to the helplines if your profile is compromised. Use social media to show how your organization is preparing.
- ☐ Raise awareness of tactics used in disinformation campaigns.
- ☐ Craft communications materials that can be used in a potential cyber disruption, including social media messages.
- ☐ Ensure that staff understand their role in a cyber disruption. For those who do not have a specific task to carry out, reassure them that their work is important and inform them how they can continue doing their jobs while designated managers handle the cyber disruption.
- ☐ Ensure that communications plans can be accessed and are regularly updated.

Action: Before a cyber crisis becomes public

- ☐ Obtain technical briefing. (Assess and verify all information.)
- ☐ Decide whether to activate technical response team(s).
- ☐ Decide whether website and social media accounts can remain online. If you must disable them, launch a microsite (hosted on a different network) in their place.
- ☐ If email is potentially compromised, use an outside communications channel such as a secure messaging app with end-to-end encryption.
- ☐ Consult appropriate government authorities.

- ☐ Meet internally in central meeting room; set internal communication schedule.
- ☐ Determine technical response team(s) roles and responsibilities, if you have not already done so.
- ☐ Determine and identify the appropriate stakeholders for the disruption response.
- ☐ Determine broad communications strategy.
- ☐ Prepare holding statement based on language you have already drafted.
- ☐ Develop communications plan.
- ☐ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).
- ☐ Establish plan for traditional and social media monitoring.
- ☐ Establish media response protocol.
- ☐ Notify employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- ☐ Notify stakeholders and galvanize support.
- ☐ Begin media (social and traditional) monitoring.

Action: Once a cyber disruption becomes public

- ☐ Fact check: Make sure communications materials reflect current facts.
- ☐ Execute rollout plan, including informing media, if appropriate.
- ☐ Determine if microsite/web page is needed.
- ☐ Record an office greeting for phone system, if necessary.
- ☐ Maintain a record of inbound media inquiries and responses, add bullets on feedback information from coverage, conversations with reporters and other data on external reaction.
- ☐ Continue media (social and traditional) monitoring.
- ☐ Review and revise messaging, as needed, based on feedback.

General Media Inquiries Checklist

Gather basic facts:

- ☐ Story topic/angle/deadline
- ☐ Platform (blog, newspaper, television, or radio) plus request content and images
- ☐ Other potential interview subjects
- ☐ Remember: Only designated spokespeople should speak or provide content.
- ☐ Remember: You have rights when you communicate with journalists, especially when asked about technical details you wouldn't be expected to know. "Let me see what I can find out for you" is always an option for a response. This may mean that you return to the reporter without any additional information. You are not obligated to provide details.
- ☐ Remember: Reporters are under pressure to produce a story and may shift the pressure to you. Do not speculate to fill gaps for them.

Notify key people:

- ☐ Meet internally.
- ☐ Craft media plan. Includes internal plans for staff and stakeholder communications.
- ☐ Designate key spokespeople and content providers. Assign tasks.
- ☐ Assist in crafting messaging. Reflect key audiences, people affected now, and those who will be affected in the future.
- ☐ Media
- ☐ Government offices
- ☐ Vendors
- ☐ General Public
- ☐ Demonstrate leadership by describing the steps you are taking to address this cyber incident. Consider contacting stakeholders who may be affected, especially if you think they may dislike or disagree with your messages.