



**IT Security Procedural Guide:
Incident Response (IR)
CIO-IT Security-01-02**

Revision 17

March 20, 2019

VERSION HISTORY/CHANGE RECORD

Revision 1 – August 12, 2005				
Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents	Various
3	Scott/Heard	Inclusion of CIO-IT Security-01-02, Handling IT Security Incident, Addendum 1	Updated to reflect Addendum 1 procedures in the master guide CIO-IT Security-01-02, Handling IT Security Incident	Various
4	Heard	Inclusion of current Federal incident identification guidelines	To ensure agency compliance	4,6 And Appendix A
Revision 2 – October 26, 2005				
1	Heard	Correct error in table of contents		lii
2	Berlas	Revised Incident Handling Form	Appropriate US Cert Form updated	Appendix A
Revision 3 – July 21, 2006				
1	Berlas	Updated references to current IT Security Policy - GSA CIO P 2100.1C	To reflect current policy	Various
2	Berlas	Updated Incident Reporting Form in Appendix A	To ensure agency compliance	Various
3	Berlas	Updated Guide to be consistent with requirements in OMB Memorandum M-06-19.	To ensure agency compliance	Appendix A
Revision 4 – March 26, 2007				
1	Berlas	Updated Incident Reporting Form in Appendix A	To ensure agency compliance	Appendix A
Revision 5 – June 28, 2007				
1	Berlas	Updated Incident Reporting Form in Appendix A	To ensure agency compliance	Appendix A
2	Berlas	Updated references to current IT Security Policy - GSA CIO P 2100.1D	To reflect current policy	Various
3	Berlas	Updated Appendix C to include the ERASER tool.	Tool is used to securely delete sensitive files related to data leakage incidents.	Appendix B
Revision 6 – April 21, 2008				
1	Hummel / Windelberg	Changes throughout the document to correspond with	The most current version of GSA CIO P 2100 and more	Various

		updated version of GSA CIO P 2100.1D and other guidance	detailed guidance on implementing policy.	
Revision 7 – August 14, 2009				
1	Berlas	Updated reference and procedures for new IR Toolkit	Updates to IR Toolkit	Various
2	Berlas	Changes throughout the document to correspond with updated version of GSA CIO P 2100.1	The most current version of GSA CIO P 2100 and more detailed guidance on implementing policy.	Various
Revision - 8 July 6, 2010				
1	Berlas / Cook	Updated 800-53 rev3 references, as well as changes throughout document.	Updates required to ensure agency compliance.	Various
Revision 9 – April 7, 2015				
1	Salamon	Updated 800-53 rev4 references, NIST SP 800-61 R2 references, updates to CIO P 2100.1, incident response testing and training, ServiceNow integration for incident management, and other process updates throughout the document	Updated to reflect updated guidance and processes	Various
Revision 10 – July 9, 2015				
1	Berlas/ Salamon	Updates Sections 2 and 4 to address specific reporting and response processes related to phishing attempts	Updated to reflect more specific processes that are in place	Various
Revision 11 – October 1, 2015				
1	Berlas/ Salamon	Updated to reflect changes in US-CERT Reporting Guidelines, FISMA law and changes in processes	Updated to reflect updated guidance and processes	Various
Revision 12 – March 15, 2016				
1	Berlas/ Salamon	Updated to reflect changes in policy, processes, and OMB guidance	Updated to reflect update to GSA CIO P 2100.1 and OMB M-16-03	Various
2	Cozart-Ramos/ Klemens	Added specific references to NIST 800-53 Rev 4 controls, formatting, technical editing.	Ensure NIST 800-53 Rev 4 controls are addressed, verify references and links, grammar/editing	Various
Revision 13 – October 11, 2016				
1	Berlas/ Salamon	Updated to clarify definition of serious incidents and process for PII incidents for lost / stolen devices.	Clarify requirements	Appendix A, 29
Revision 14 – April 3, 2017				
1	Berlas/ Salamon	Updated to reflect changes to US-CERT incident reporting requirements and definition of major incidents	Updated reporting and major incident requirements	Various
2	Berlas/	Created Section 4.7 for lost /	Created to reflect process	35

	Salamon	stolen incidents	changes	
Revision 15 – September 14, 2017				
1	Berlas/ Salamon	Updated to clarify when to call the incident response team	Updated reporting and major incident requirements	36
2	Berlas/ Salamon	Clarified process for escalating serious incidents by phone or email	Feedback from reviewer	Various
3	Berlas/ Salamon	Updated references from M-07-16 to M-17-12	Feedback from reviewer	Various
Revision 16 – March 22, 2018				
1	Berlas/ Salamon	Clarifies that unsuccessful incidents are not required to be reported	Clarification of process	19
2	Berlas/ Salamon	Added language regarding data exfiltration monitoring	Document existing process for data exfiltration monitoring	22
3	Berlas/ Salamon	Updated to reflect Insider Threat Program reporting	Updated reporting request from OMA for Insider Threats	36
4	Berlas/ Salamon	Explicitly identifies that the IR Team is the Incident Commander	FISMA reporting updates	3, 36
Revision 17 – March 20, 2019				
1	Speidel	Updated to include PII incident report template, checklist and breach determination and notification timeframe	Updates to process	Various
2	Salamon	New reporting requirements for sending incidents to Contracting Officer	Updates to process	21, 36
3	Salamon	Updates to major incident handling	Updates to process and OMB reporting definitions	Various
3	Salamon	Updates for tools in use	Updates to process	Appendix C

Approval

IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02, Revision 17, is hereby approved for distribution.

3/20/2019

X Bo Berlas

Bo Berlas

Acting GSA Chief Information Security Officer

Signed by: General Services Administration

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE) at gsa-ir@gsa.gov

Table of Contents

1	Introduction	1
1.1	Purpose.....	2
1.2	Policy.....	2
1.2.1	Policies Regarding Contractors and Contractor Facilities	4
1.3	Incident Response Roles and Responsibilities.....	4
2	Federal Incident Reporting Guidelines.....	10
2.1	US-CERT Impact Classifications.....	10
2.2	US-CERT Threat Vectors.....	13
2.3	US-CERT Cause Analysis.....	15
2.4	US-CERT Incident Attributes	16
2.5	Major Incident Definition and Requirements.....	18
2.5.1	A Privacy Breach that Constitutes a Major Incident	19
2.5.2	Congressional Reporting of Major Incidents	19
2.5.3	Congressional Reporting of a Privacy Breach	20
3	Incident Reporting Process	20
3.1	How to Report IT Security Incidents	21
3.1.1	General Incident Reporting.....	21
3.1.2	Incident Reporting for Externally Hosted Information Systems.....	21
3.1.3	Incident Reporting for Vendor Identified Incidents (Including GSA Leases)	22
3.2	OCISO’s Incident Reporting Responsibilities	22
3.3	OCISO’s Threat Awareness Program	23
4	Incident Response Process	23
4.1	Tier 1: Initial Determination and Reporting	26
4.1.1	Tier 1 Response Tasks	27
4.2	Tier 2: Follow-up and Restoration	28
4.2.1	Tier 2 Response Tasks	28
4.3	Tier 3: Investigation and Counteraction	29
4.3.1	Tier 3 Response Tasks	29
4.4	Incident Response Plan Testing and Exercises	31
4.5	Incident Response Plan Training.....	31
4.6	Incident Response for Phishing Attempts	32
4.6.1	Differences between Phishing Attempt, Spam, and Social Engineering	32
4.6.2	Identification Standards for Reporting Phishing Attempts to US-CERT.....	32
4.6.3	User Communications.....	33
4.6.4	Response Process for GSA Incident Response Team	33
4.7	Incident Response for Lost / Stolen Devices, PIV Cards, or Tokens	35
4.8	Incident Response for PII.....	35
5	How Does the OCISO Respond to Serious Incidents?	36
5.1	Step 1: Verify the Source	36
5.2	Step 2: Verify the Incident	36
5.3	Step 3: Notify Other Parties.....	36

5.3.1 US-CERT.....	36
5.3.2 Other Organizations.....	36
5.3.3 GSA Management.....	36
5.3.4 GSA Inspector General.....	36
5.3.5 Reporting Major Incidents to U.S. Congress.....	37
5.3.6 Reporting Incidents to the Office of Mission Assurance’s Insider Threat Program.....	37
5.3.7 Reporting Incidents to the Contracting Officer.....	37
5.4 Step 4: Form Incident Handling Team.....	38
5.5 Step 5: Gather Evidence.....	38
5.6 Step 6: Contain, Eradicate and Recover from the Incident.....	38
5.7 Step 7: Follow-up after the Incident is Resolved.....	39
6 Best Practices.....	39
6.1 Key Questions to Ask.....	39
6.1.1 Is it an incident or a false positive?.....	39
6.1.2 Is the incident still in progress?.....	39
6.1.3 What is its extent of the incident? Does it involve more than one device?.....	40
6.1.4 Why is it in this particular device and how did it get there?.....	40
7 Live Response Process.....	40
8 Summary.....	41
APPENDIX A - Glossary of Terms.....	42
APPENDIX B – GSA Cyber Incident Reporting Form Instructions.....	44
APPENDIX C – Incident Response and Handling Tools.....	45

Table of Figures and Tables

Table 1: Federal Agency Incident Impact Classifications.....	11
Table 2: Federal Threat Vector Taxonomy.....	14
Figure 1: Threat Vector Decision Tree.....	15
Figure 2: Incident Handling, Response, and Reporting Swimchart.....	26
Table 3: Incident Types.....	27
Table 4: Mapping of NIST IR Controls to GSA Documents.....	41

1 Introduction

An “incident” or “information security incident” can be thought of as a violation or imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices. An incident response capability is therefore necessary to:

- Rapidly detect imminent threats or incidents;
- Prevent, stop or minimize loss and destruction;
- Mitigate the weaknesses exploited;
- Restore Information Technology (IT) services;
- Investigate incidents for root causes and/or forensic evidence;
- Report incident to United States Computer Emergency Readiness Team (US-CERT) and/or other responsible federal authorities; and
- Document the incident and General Services Administration (GSA’s) response to it.

The implementation of an Incident Response (IR) capability is critical to the protection of GSA’s information and IT assets. When fully implemented with the appropriate tools, procedures, and processes, the response to a security incident can significantly reduce the potential impact of an incident to GSA’s information, IT resources and individuals. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

This guide presents GSA’s policy, procedures, and processes for incident response. It defines mandatory reporting requirements to the US-CERT when the confidentiality, integrity, or availability of a Federal Government information system has been confirmed as compromised. It also outlines the reporting process for external reporting to the GSA Office of Inspector General (OIG) and U.S. Congress. Incident reporting to US-CERT aligns with updated US-CERT Federal Incident Notification Guidelines. This guide details three incident handling processes and the associated roles and responsibilities. Section 3 explains how to report IT security incidents. Section 4 explains the incident response process, and breaks it down into three tiers. Tier 1 processes consist of determining if an incident has occurred and reporting the incidents or suspected incidents. Tier 2 processes consist of activities related to following up with an actual response through the restoration of services. Tier 3 processes consist of the investigation and any counteractions. Section 5 explains how the Office of the Chief Information Security Officer (OCISO) responds to incidents that are deemed serious.

Every Service and Staff Office must be covered by a documented and tested incident handling process to address Tier 1 and Tier 2 incident response for systems under their jurisdiction. The office receiving the initial report is responsible for distributing information within GSA, identifying supporting resources needed, and if appropriate, addressing the incident. The OCISO in consultation with the reporting office will determine whether legal counsel or law enforcement involvement is warranted. The final decision to notify such entities is the responsibility of the OCISO, with notification to the GSA CIO. Within the OCISO, the GSA Security Engineering Division’s (ISE) Incident Response Team is responsible for tracking incidents, reporting incidents to US-CERT and to the OIG, and coordinating response efforts for incidents that require additional resources for remediation.

The incident response principles and practices described in this guide are based on guidance from the National Institute of Standards and Technology (NIST) including [NIST Special Publication \(SP\) 800-61 Revision 2](#), “Computer Security Incident Handling Guide,” and [NIST SP 800-53 Revision 4](#), “Security and Privacy Controls for Federal Information Systems and Organizations,” and the updated US-CERT Federal Incident Notification Guidelines. This guide provides procedures for incident response, roles and responsibilities, NIST SP 800-53 incident response requirements per FIPS 199 impact level and procedures for implementing these requirements, and related best practices.

1.1 Purpose

This IT Security Procedural Guide: *Incident Response* defines IR requirements as identified in [GSA Order CIO 2100.1](#), “GSA Information Technology (IT) Security Policy”, [CIO 9297.2C](#), “GSA Information Breach Notification Policy”, and NIST SP 800-53, and US-CERT Federal Incident Notification Guidelines. This guide provides specific procedures for GSA employees and contractors with significant security responsibilities to follow for implementing the IR functions for systems.

1.2 Policy

GSA CIO 2100.1, Chapter 6, Policy for Respond Function, states:

1. Response planning.
 - a. *All information systems must have their contingency plans and Incident Response Plans tested annually.*
 - b. *Lessons learned during contingency plan and incident response plan tests must be incorporated into revised plans.*
2. Communications.
 - a. *GSA employees and contractors on the Incident Response Team identified in GSA CIO-IT Security-01-02 are trained on their roles and responsibilities within 60 days of assignment and annually thereafter.*
 - b. *Personnel with contingency planning responsibilities must be trained in their contingency roles and responsibilities with respect to the information system annually.*
 - c. *Users must immediately report suspected vulnerabilities, security violations, and security incidents to the GSA IT Service Desk.*
 - d. *Users must immediately report lost or stolen portable storage devices to the GSA IT Service Desk.*
 - e. *All incidents involving the loss or theft of GSA hardware, software, and/or information in physical form must be reported immediately to the GSA IT Service Desk.*
 - (1) *Users must also report all losses to the Federal Protective Service (FPS) via the appropriate Regional Hotline, as directed by the appropriate ISSO or the GSA IT Service Desk.*

- (2) Users must also report any loss that occurs outside of Federal facilities to the local police.*
 - (3) Lost PIV cards must be reported to the Central or Regional OMA office after reporting to the GSA IT Service Desk.*
 - f. GSA Incident Response Teams must report incidents as described in GSA CIO-IT Security-01-02. FISMA requires "major incidents" to be reported to the U.S. Congress within seven days of detection.*
 - g. Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to PII, whether physical or electronic) shall also follow reporting and response procedures as defined in GSA Order CIO 9297.2C.*
 - h. ISSOs must report any security incidents reported to them to the GSA IT Service Desk and GSA OCISO.*
 - i. Information will be shared by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.*
 - j. Coordination with stakeholders will be conducted by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.*
 - k. Information sharing with external stakeholders will be conducted by the GSA Incident Response Team, as appropriate and in coordination with the GSA CISO, IAW GSA CIO-IT Security-01-02.*
- 3. Analysis.**
- a. The OCISO will communicate notifications/alerts from detection systems for investigation by GSA's Incident Response Team via email or the GSA IT Service Desk. Procedures must be documented for responses to detected irregularities.*
 - b. The GSA Incident Response Team will investigate notifications/alerts from detection systems IAW GSA CIO-IT Security-01-02.*
 - c. The GSA Incident Response Team will determine the impact of an incident in coordination with other personnel/organization, as appropriate, during the investigation process defined in GSA CIO-IT Security-01-02.*
 - d. The GSA Incident Response Team will perform forensics analysis of incidents/the evidence of incidents, as necessary, to support investigations as described in GSA CIO-IT Security-01-02.*
 - e. The GSA OCISO and Incident Response Team will categorize incidents IAW GSA CIO-IT Security-01-02.*
 - f. The OCISO will establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning.*
 - g. The OCISO will notify personnel with security responsibilities of vulnerabilities disclosed via security advisory alerts or other external sources.*
 - h. ISSMs and ISSOs must report on the status of security advisory alerts to the Office of the CISO upon request.*

4. Mitigation.

- a. *The GSA Incident Response Team, in coordination with system personnel, will contain incidents IAW GSA CIO-IT Security-01-02.*
 - b. *Incidents will be mitigated or remediated based on activities executed by the GSA Incident Response Team and system personnel, as described in GSA CIO-IT Security-01-02 and the system's recovery plan.*
 - c. *IAW GSA CIO-IT Security-06-30, newly identified vulnerabilities must be:*
 - (1) *Remediated or mitigated IAW specified timeframes;*
 - (2) *Included in a Plan of Action & Milestones; or*
 - (3) *Included in an Acceptance of Risk Letter.*
5. **Improvements.**
- a. *Incident response plans must be updated based on lessons learned during incident response or plan testing.*
 - b. *Contingency plans must be updated based on lessons learned during responses to disasters, other events invoking the contingency plan or plan testing.*
 - c. *Incident response strategies must be reviewed and updated, if necessary, at least annually to address system/organizational changes and problems or issues encountered while responding to incidents or plan testing.*

1.2.1 Policies Regarding Contractors and Contractor Facilities

Contractors and other entities that process and host GSA information are bound by GSA CIO 2100.1, the terms of their contracts, and [Federal Information Security Modernization Act \(FISMA\) of 2014, Section 3551](#) to protect the security of this information, including the support of incident response efforts.

Refer to GSA CIO 2100.1 for a detailed listing of incident handling related policies.

1.3 Incident Response Roles and Responsibilities

There are many roles associated with implementing an effective incident response capability. System Owners and System Program Managers/Project Managers have a direct responsibility to ensure the implementation of the IR process. The System Owners for each information system are responsible for ensuring that an IR process has been implemented for their respective Service/Staff Office (S/SO) systems and that the appropriate people have been assigned IR related roles and responsibilities. The System Program Managers/Project Managers have direct responsibility to ensure effective implementation and management of GSA's IR requirements for each of their systems. The GSA Incident Response Team is empowered to be the *Incident Commanders*, responsible for directing and managing GSA cybersecurity incidents in accordance with [FY 2018 CIO FISMA Metrics](#).

This section highlights the roles and responsibilities related to implementation of the IR process. The roles and responsibilities outlined in this document are not all-inclusive. The roles and responsibilities are defined fully in the GSA CIO 2100.1 and GSA CIO 9297.2.

GSA Chief Information Officer (CIO). Incident Response related responsibilities of the CIO include the following:

- Ensuring information assurance and the protection of GSA's cyber-based critical infrastructure;
- Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.

Chief Information Security Officer (CISO). Incident Response related responsibilities of the CISO include the following:

- Reporting to the GSA CIO on activities and trends that may affect the security of systems and applications assigned to GSA;
- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy;
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices;
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- Developing and implementing procedures for detecting, reporting, and responding to security incidents;
- Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of GSA.

Authorizing Official (AO). Incident Response related responsibilities of the AO include the following:

- Ensuring adherence to GSA's IT Security Policy;
- Ensuring all incidents involving data breaches which could result in identity theft are coordinated through GSA IT's Office of the Chief Information Security Officer (OCISO) and the GSA Management Incident Response Team (MIRT) using the GSA breach notification plan per [OMB Memorandum M-17-12](#), "Preparing for and Responding to a Breach of Personally Identifiable Information," IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02 (this guide) and GSA Order, [CIO 9297.2C](#), "GSA Information Breach Notification Policy";

Information Systems Security Manager (ISSM). Incident Response related responsibilities of the ISSM include the following:

- Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security training, incident reports, contingency plan testing, and other IT security program issues.

Information Systems Security Officer (ISSO). Incident Response related responsibilities of the ISSO include the following:

- Ensuring the system is operated, used, maintained, and disposed of in accordance with internal security policies and procedures. Necessary security controls should be in place and operating as intended;
- Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk;
- Assisting System Owners in completing and maintaining the appropriate security documentation including the system security plan;
- Identifying, reporting and responding to security incidents;
- Reviewing and responding as appropriate to Security Advisory Alerts on vulnerabilities.
- Reviewing system security audit trails and system security documentation to ensure security measures are implemented effectively;
- Evaluating known vulnerabilities to ascertain if additional safeguards are needed; ensuring systems are patched, and security hardened;
- Beginning protective or corrective measures if a security breach occurs;
- Assisting in the development and maintenance of contingency plan and contingency plan test report documentation.

System Owners. Incident Response related responsibilities of the System Owners include the following:

- Ensuring their systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM;
- Participating in activities related to the assessment and authorization of the system to include security planning, risk assessments, security and incident response testing, and contingency planning and testing;
- Developing, implementing, and maintaining an approved IT Contingency Plan which includes an acceptable Business Impact Analysis (BIA);
- Coordinating with IT security personnel including the ISSM and ISSO and Data Owners to ensure implementation of system and data security requirements;
- Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities;
- Working with Data Owners to ensure that log data is archived for a period of not less than 180 days;
- Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities;
- Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

Data Owners (a.k.a. Functional Business Line Managers). Incident Response related responsibilities of the Data Owners include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.
- Ensuring protection of GSA's systems and data in accordance with GSA's IT Security Policy and the GSA Records Management Program.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements;
- Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.
- Working with the System Owner to ensure that log data is archived for a period of not less than 180 days;
- Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities;
- Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.
- Working with the System Owner to provide the initial Agency Response Team (IART) evidence that it has provided any required breach notification and/or services within the required timeframe.

Acquisitions/Contracting (Contracting officers [CO]/Contracting Officer's Representatives [COR]). Incident Response related responsibilities of Acquisitions/Contract include the following:

- Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy;
- Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency's information security policy;
- Ensuring that all IT acquisitions include the appropriate security requirements in each contract and task order;
- Ensuring all GSA contracts, Request for Proposals (RFP), and Request for Quotes (RFQ) involving Privacy Act information adhere to the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1) and include the specified contract clauses (Parts 52.224-1 and 52.224-2), as appropriate;
- Ensuring new solicitations where the information system is contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency) includes the security contract language from [IT Security Procedural Guide CIO-IT Security 09-48](#), "Security Language for IT Acquisition Efforts".

- Working with the System Owner to provide the IART evidence that it has provided any required breach notification and/or services within the required timeframe.

Custodians. Incident Response related responsibilities of the Custodians include the following:

- Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected;
- Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner;
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the Authorizing Official.

Users of IT Resources. Incident Response related responsibilities of Users of IT Resources include the following:

- Reporting any observed or suspected security problems/incidents to their local IT Service Desk.

System/Network Administrators. Incident Response related responsibilities of System/Network Administrators include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines;
- Implementing system backups and patching of security vulnerabilities;
- Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented;
- Identifying and reporting security incidents and assisting the OCISO in resolving the security incident.

Initial Agency Response Team. Incident Response related responsibilities of the Initial Agency Response Team include the following:

- Breaches that involve a limited number of individuals and a limited amount of breached PII will be considered minor. Breaches that impact up to 1,000 individuals will be handled by the Initial Agency Response Team.
- The Chief Privacy Officer leads this group and assists the program office by providing a notification template, information on identity protection services (if necessary) and any other assistance deemed necessary.
- Within the required timeframe of an incident being escalated to it, the Initial Agency Response Team is responsible for both confirming whether a breach in fact occurred and assisting the program office as it provides any breach notification and/or services to the impacted individuals.
- The OCISO is responsible for ensuring the US-CERT Report is submitted and the Office of Inspector General (OIG) is notified. The Initial Agency Response Team will determine the appropriate remedy. If a unanimous decision cannot be made, it will be elevated to the Full Agency Team.

- The program office is responsible for providing the remedy to the impacted individuals (including associated costs). It will also provide evidence that notification was provided to impacted individuals within ninety (90) calendar days of the date of the incident's escalation to the Initial Agency Response Team, absent national security or law enforcement agency involvement, an incident or breach implicating large numbers of records or affected individuals, or similarly exigent circumstances. The SAOP will determine the appropriate timeframe for incidents not escalated to the Full Response Team (see below).
- If the impacted individuals are contractors, notification will be handled by the contract officer, working with the vendor. The Chief Privacy Officer will provide a notification template and other assistance deemed necessary.
- The Senior Agency Official for Privacy (SAOP) is the SES responsible for the privacy program at GSA. The Chief Privacy Officer handles the management and operation of the privacy office at GSA.

Full Response Team. Incident Response related responsibilities of the Full Response Team include the following:

- A major breach involves a large amount of PII. Breaches that impact more than 1,000 individuals or significant types of PII will be deemed as "major" and will be handled by the Full Response Team. Based on the risk assessment, breaches that impact fewer than 1,000 may still be moved under the purview of the Full Response Team should they involve a large amount of PII or that may cause substantial harm, embarrassment, inconvenience, or unfairness to any individual.
- This team consists of the program manager of the program experiencing or responsible for the breach, the SAOP, the Chief Information Officer (CIO), OCISO, Chief Privacy Officer, Office of Strategic Communications (OSC), Office of Congressional and Intergovernmental Affairs (OCIA), and the Office of General Counsel (OGC), Mission or system owners, Security Engineering Division Director or representative.
- Within the required timeframe of an incident being escalated to it, the Full Response Team is responsible for both confirming whether a breach in fact occurred and assisting the program office as it provides any notification and/or services to the impacted individuals absent national security or law enforcement agency involvement, an incident or breach implicating large numbers of records or affected individuals or similarly exigent circumstances. The Full Response Team will determine the appropriate timeframe for breaches under its purview.
- The Full Response Team is designed as the team that is required per the current [OMB Memorandum](#) providing Guidance on Federal Information Security and Privacy Management Requirements and is tasked with responsibility for the determining whether a major incident has occurred (requiring Congressional and Inspector General reporting). The CISO will lead for major non-privacy incident determinations and the SAOP will lead for major privacy incident determinations.

2 Federal Incident Reporting Guidelines

The US-CERT coordinates defense against and responses to cyber-attacks. Notifying US-CERT of a computer security incident is mandatory when the confidentiality, integrity, or availability of a Federal Government information system has been potentially compromised. Notification of incidents which have no potential functional or information impact such as passive scans, attempted access, or thwarted exploits may be submitted to US-CERT voluntarily. However, US-CERT has asked that encrypted lost or stolen devices and unsuccessful phishing attempts¹ no longer be reported to US-CERT as incidents. US-CERT has updated its [reporting requirements](#) to the following:

Requirement: *Agencies must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to the NCCIC/US-CERT with the required data elements, as well as any other available information, **within one hour** of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department. In some cases, it may not be feasible to have complete and validated information for the section below (Submitting Incident Notifications) prior to reporting. Agencies should provide their best estimate at the time of notification and report updated information as it becomes available. Events that have been found by the reporting agency not to impact confidentiality, integrity or availability may be reported voluntarily to US-CERT; however, they may not be included in the FISMA Annual Report to Congress.*

GSA will put forth a best effort to report all mandatory incidents within one-hour of notification to the GSA Incident Response Team and provide all available information. GSA will not delay reporting in order to provide further details (i.e. root cause, vulnerabilities exploited, or mitigation actions taken) as this may result in high risk to the system or enterprise. If the cause of the incident is later identified, the threat vector may be updated in a follow-up report.

US-CERT has directed agencies to determine their own thresholds for identifying “potential” impact to confidentiality, integrity or availability. Based on this guidance, the GSA Incident Response Team will define potential incidents as those in which there is reason to suspect that an impact to confidentiality, integrity, or availability has occurred or will occur imminently. This would exclude the reporting of vulnerabilities in which there is no evidence of exploitation (i.e. a vulnerable condition). Common scenarios handled by the GSA Incident Response team and the scenarios in which reporting requirements are triggered are documented in Incident Response Standard Operating Procedures.

2.1 US-CERT Impact Classifications

Incidents may affect multiple types of data. Therefore, when classifying an incident GSA may select multiple options to identify the information impact. Incidents with a potential functional,

¹ Unsuccessful phishing attempts may be sent to phishing-report@us-cert.gov, in which there will be an automated process for US-CERT to extract indicators and the GSA IR team will voluntarily do this, as detailed in Section 4.6.

information, or recovery impact must be IMMEDIATELY reported to the GSA IT Service Desk and the OCISO. Details of the reporting process are explained in Section 3. Use **Table 1** below to identify the impact of the incident. The term “classified information” is defined in IAW [CNSSI 4009](#). The term “proprietary information” is defined in IAW NIST SP 800-61. The term “personally identifiable information” is defined IAW with OMB Memorandum [M-17-12](#).

Note: Incidents involving non-cyber PII exposures or classified data spillage (i.e. unsecured hard copies) will not be reported to US-CERT. The GSA Senior Agency Official for Privacy (SAOP) will coordinate all response efforts related to non-cyber incidents involving PII.

Table 1: Federal Agency Incident Impact Classifications

Impact Category	Category Severity Levels
Functional Impact – A measure of the impact to business functionality or ability to provide services	NO IMPACT – Event has no impact.
	NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
	MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to non-critical systems and services.
	MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
	SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.
	DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
	SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
	DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.

Impact Category	Category Severity Levels
Information Impact – Describes the type of information lost, compromised, or corrupted.	NO IMPACT – No known data impact.
	SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
	PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII) ² or personal health information (PHI) was compromised.
	PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information ³ , such as protected critical infrastructure information (PCI), intellectual property, or trade secrets was compromised.
	DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
	CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated.
	CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
	DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.
Recoverability – Identifies the scope of resources needed to recover from the incident	REGULAR – Time to recovery is predictable with existing resources.
	SUPPLEMENTED – Time to recovery is predictable with additional resources.
	EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

The Federal Agency Incident Impact Classification table is available on the [US-CERT website](#).

² As defined in OMB Memorandum M-17-12, “personally identifiable information” refers to “information which can be used to distinguish or trace an individual's identity.

³ As defined by NIST, “proprietary information” is “information that is not public knowledge and that is viewed as the property of the holder, with the holder of that information responsible to declare it and treat it as proprietary”.

** Per [OMB M-17-12](#), Preparing for and Responding to a Breach of Personally Identifiable Information , the term PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual.. However, incidents involving non-cyber PII exposures or classified data spillage (i.e. unsecured hard copies) should not be reported to US-CERT and will be reported to GSA's Privacy Office as required by policy, consistent with updated federal incident reporting guidelines.

*** GSA Policy specifies that all mobile data storage devices (including laptop hard drives, USB external disk or Flash storage, etc.) must be encrypted with a FIPS 140-2 certified encryption module. If a device is lost or stolen that violates this policy or the keys that protect the device could be recovered, the incident must be treated as an incident with information impact and reported immediately as such. In addition, US-CERT has requested that simple loss or theft of PIV card without any attempts for unauthorized usage shall not be reported as an incident but must be reported to the Regional Office of Mission Assurance (OMA) office, as directed by the GSA IT Service Desk staff.

**** Phishing attempts reported to the GSA Incident Response Team will be reported to US-CERT as follows:

- Phishing attempts where ENT domain credential or credentials to other GSA systems are used to gain unauthorized access; or results in malicious code being successfully executed on a GSA server or workstation will be reported with the appropriate functional, information, and/or recoverability impact classification.
- Sensitive information revealed via a spear phishing email or other means will also be reported as an incident with the appropriate information and recoverability impact classification.
- Per direction from US-CERT, other phishing attempts will not be reported as incidents, but submitted separately to phishing-report@us-cert.gov in accordance with Section 4.6. However, the GSA Incident Response Team, at its option, may choose to report unsuccessful phishing incidents as deemed necessary.

2.2 US-CERT Threat Vectors

To clearly communicate incidents throughout the Federal Government and supported organizations, it is necessary for government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the Federal Government should use the common taxonomy outlined in Table 2.

Table 2 is a high-level set of concepts and descriptions developed from guidance in NIST SP 800-61 Revision 2. GSA, as a Federal civilian agency, must utilize the following threat vectors taxonomy when sending cybersecurity incident notifications to US-CERT. US-CERT provides the following guidance for use this table:

Note: Incidents may affect multiple types of data; therefore, D/As may select multiple options when identifying the information impact. The security categorization of federal information and information systems must be determined in accordance with Federal Information Processing Standards (FIPS) Publication 199. Specific thresholds for loss-of-service availability (e.g., all, subset, loss of efficiency) must be defined by the reporting organization. Contact your Security Office for guidance on responding to classified data spillage.

Table 2: Federal Threat Vector Taxonomy

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector	

2.3 US-CERT Cause Analysis

The decision tree shown in Figure 1 is used to identify the appropriate threat vector:

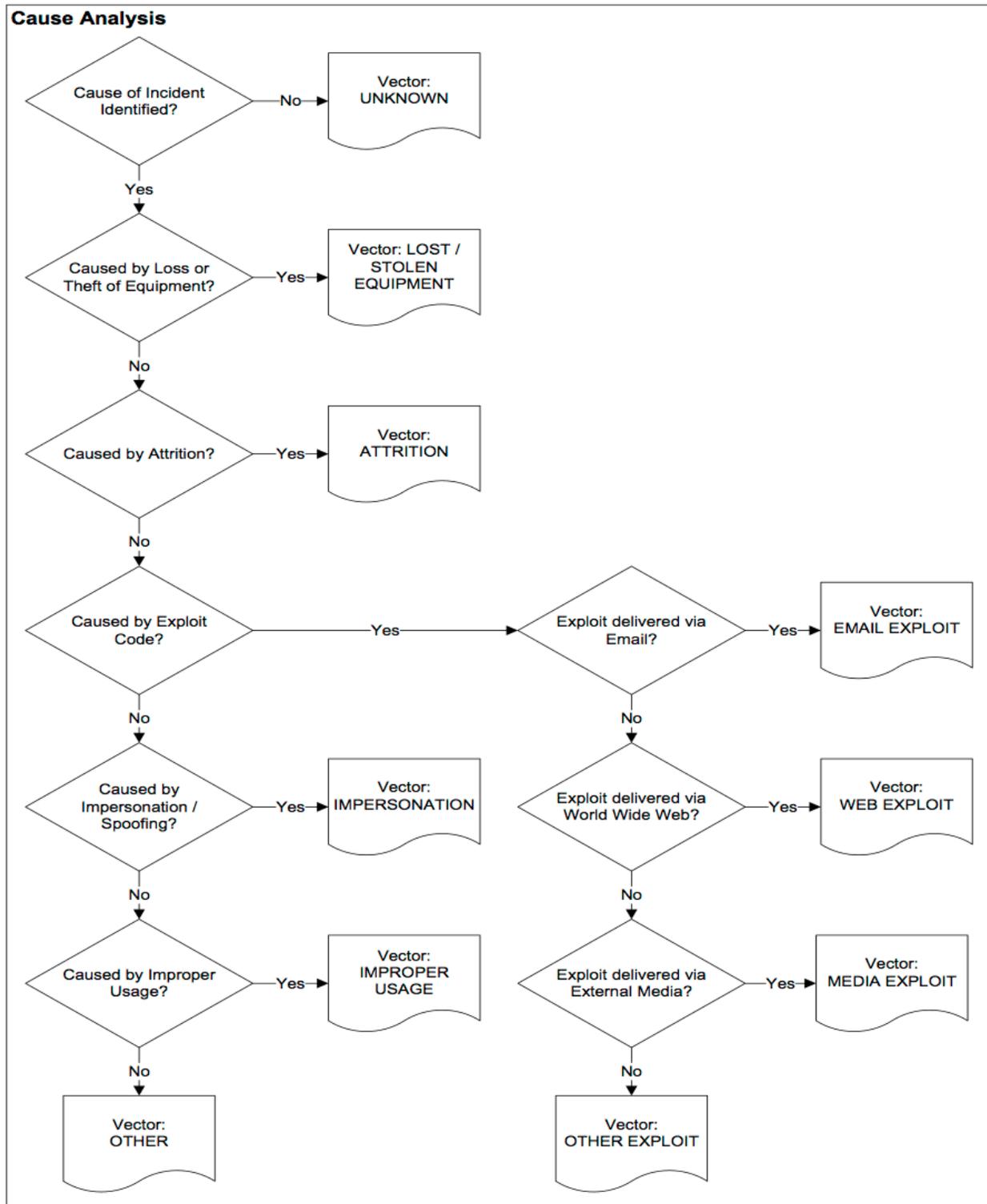


Figure 1: Threat Vector Decision Tree

2.4 US-CERT Incident Attributes

To support the assessment of national-level severity and priority of cyber incidents, including those affecting private-sector entities, the US-CERT's National Cybersecurity & Communications Integration Center (NCCIC) will analyze the following incident attributes utilizing the NCCIC Cyber Incident Scoring System (NCISS):

- Functional Impact,
- Information Impact,
- Recoverability,
- Location of Observed Activity
- Observed Activity,
- Actor Characterization,
- Cross-Sector Dependency, and
- Potential Impact.

US-CERT Note: Agencies are not required or expected to provide Actor Characterization, Cross-Sector Dependency, or Potential Impact information. These are assessed independently by NCCIC/US-CERT incident handlers and analysts. Additionally, Observed Activity is not currently required and is based on the attack vector, if known, and maps to the Office of the Director of National Intelligence's (ODNI) Cyber Threat Framework.

This information will be utilized to calculate a severity score according to the NCISS. The NCISS aligns with the priority levels of the Cyber Incident Severity Schema (CISS):

- **Emergency (Black):** Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.
- **Severe (Red):** Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
- **High (Orange):** Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Medium (Yellow):** May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Low (Green):** Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Baseline – Minor (Blue):** Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Baseline – Negligible (White):** Unsubstantiated or inconsequential event.

The following incident attribute definitions are taken from the NCCIC NCISS.

Attribute Category	Attribute Definitions
<p>Location of Observed Activity: Where the observed activity was detected in the network.</p>	<p>LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network’s demilitarized zone (DMZ)</p>
	<p>LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.</p>
	<p>LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores.</p>
	<p>LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay “jump” boxes into more critical systems.</p>
	<p>LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.</p>
	<p>LEVEL 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments.</p>
	<p>LEVEL 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.</p>
	<p>UNKNOWN – Activity was observed, but the network segment could not be identified.</p>
<p>Actor Characterization</p>	<p>The type of actor(s) involved in the incident (if known). This element is not selected by the reporting entity.</p>
<p>Cross-Sector Dependency</p>	<p>A weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA). This element is not selected by the reporting entity.</p>
<p>Potential Impact</p>	<p>An estimate of the overall national impact resulting from a total loss of service from the affected entity. This element is not selected by the reporting entity.</p>

US-CERT Note: Agencies are not required or expected to provide Actor Characterization, Cross-Sector Dependency, or Potential Impact information. These are assessed independently by NCCIC/US-CERT incident handlers and analysts. Additionally, Observed Activity is not currently

required and is based on the attack vector, if known, and maps to the ODNI Cyber Threat Framework.

2.5 Major Incident Definition and Requirements

FISMA requires the Office of Management and Budget (OMB) to define a major incident and directs agencies to report major incidents to Congress within 7 days of identification. OMB M-19-02 defines a major incident as EITHER:

Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.⁴ Agencies should determine the level of impact of the incident by using the existing incident management process established in [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-61](#), “Computer Security Incident Handling Guide.”

OR,

A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.⁵

Agencies should determine the level of impact of the incident by using the existing incident management process established in NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, and are encouraged to use the US-CERT NCISS, which is outlined in Section 2.4. Appropriate analysis of the incident will be done by the Full Response Team (see Section 1.3 for details), which will be led by the CISO for major non-privacy incidents and the SAOP for major PII incidents. The definition above leverages the NCISS and therefore creates uniformity in terminology and criteria utilized by agencies and the US-CERT incident responders.

According to US-CERT, the impacted agency is ultimately responsible for determining if an incident should be designated as major and may consult with US-CERT to make this determination. Additionally, if the NCCIC/US-CERT determines that an incident meets the

⁴ Using the NCCIC’s Cyber Incident Scoring System, this includes Level 3 events (orange), defined as those that are “likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence”; Level 4 events (red), defined as those that are “likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties”; and Level 5 events (black), defined as those that “pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons.”

⁵ The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to [OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information](#), which describes breach reporting requirements.

criteria for High (Orange) on the Cyber Incident Severity Schema (see Section 2.4), it will suggest that the agency designate that incident as a major incident. Other incidents can be escalated at the GSA Incident Response Team's discretion. GSA's response process for identifying and reporting major incidents is detailed in Section 5.3.5.

2.5.1 A Privacy Breach that Constitutes a Major Incident

According to M-19-02 a privacy breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is 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.⁶ An unauthorized modification of,⁷ unauthorized deletion of,⁸ unauthorized exfiltration of,⁹ or unauthorized access to¹⁰ 100,000 or more individuals' PII constitutes a "major incident."

2.5.2 Congressional Reporting of Major Incidents

According to M-19-02 agencies must notify appropriate Congressional Committees per FISMA 2014 of a "major incident" no later than seven (7) days after the date on which the agency determined that it has a reasonable basis to conclude that a "major incident" has occurred.¹¹ This report should take into account the information known at the time of the report, the sensitivity of the details associated with the incident, and the classification level of the information. When a "major incident" has occurred, the agency must also supplement its initial seven (7) day notification to Congress with pertinent updates within a reasonable period of time after additional information relating to the incident is discovered. This supplemental report must include summaries of:

- The threats and threat actors, vulnerabilities, and impacts relating to the incident;
- The risk assessments conducted of the affected information systems before the date on which the incident occurred;
- The status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
- The detection, response, and remediation actions.

Although agencies may consult with DHS US-CERT on whether an incident is considered a "major incident," it is ultimately the responsibility of the impacted agency to make this determination.

⁶ *The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to OMB's guidance on preparing for and responding to a breach of PII.*

⁷ *Unauthorized modification is defined as the act or process of changing components of information and/or information systems.*

⁸ *Unauthorized deletion is defined as the act or process of removing information from an information system.*

⁹ *Unauthorized exfiltration is defined as the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.*

¹⁰ *Unauthorized access is defined as the act or process of logical or physical access without permission to Federal agency information, information system, application, or other resource.*

¹¹ *This reporting is limited to the time after major incident determination and not just the detection of the incident, it is expected that an agency will take some time to determine if an incident or breach reaches the threshold to be considered "major".*

2.5.3 Congressional Reporting of a Privacy Breach

According to M-19-02, agencies must notify appropriate Congressional Committees per FISMA 2014 no later than seven (7) days after the date on which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. In addition, agencies must also supplement their initial seven (7) day notification to Congress with a report no later than 30 days after the agency discovers the breach. This supplemental report must include:

- A summary of information available about the breach, including how the breach occurred, based on information available to agency officials on the date which the agency submits the report;
- An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals, based on information available to agency officials on the date on which the agency submits the report;
- A description of any circumstances necessitating a delay in providing notice to affected individuals; and
- An estimate of whether and when the agency will provide notice to affected individuals.

3 Incident Reporting Process

Reporting is necessary to alert other organizations within GSA and the US Government of an information security threat. Reporting ensures that the response and support is commensurate with the threat. As such, it meets two objectives 1) notifying the OCISO and 2) submitting an incident report for follow-on reporting to the US-CERT, the OIG, and the US Congress, as applicable.

Initiation of the reporting process is the responsibility of any person, staff, or contractor who observes suspicious security activities that involve GSA data or IT systems. GSA contractors and outsourced IT services must have a documented incident reporting process that follows the steps outlined in Section 3.1 and Section 3.2.

Any incident with a functional, information, or recovery impact, must be reported IMMEDIATELY to the GSA IT Service Desk¹². NEVER assume that someone else has already reported the incident. The risk of an unreported incident far outweighs the possibility that an incident is reported more than once. Incidents detected by the GSA Incidents Response Team will be reported directly to US-CERT. Non-serious incidents without functional, information, or recovery impact (e.g. casual misuse) that are addressed locally should also be reported to GSA IT Service Desk as soon as possible. Incidents deemed non-serious could be pre-cursors to larger and more serious incidents. It is important for ALL IT Security incidents to be reported to the GSA IT Service Desk.

¹² *If the incident is serious (see definition in Appendix A) and immediate response from the incident response team, see Section 3.1 for escalation procedures.*

GSA does not require unsuccessful incidents with no impact to the functional, information, or recovery impact to be reported to the GSA IT Service Desk. This includes incidents where the technical control mechanisms (e.g., firewalls) performed as expected without degradation to services. However, unsuccessful incidents can always optionally be reported if the team would like another set of eyes for whatever reason, such as persistence of attempts or an inclination it is part of something bigger. In such cases, the GSA Incident Response Team will correlate against any other threat intelligence or GSA metadata, including optional reporting to US-CERT.

3.1 How to Report IT Security Incidents

This section outlines the steps for generally reporting incidents, as well as special instructions for reporting incidents for externally hosted Information Systems and for vendor-identified incidents (including GSA leases).

3.1.1 General Incident Reporting

When documenting an incident, print or capture (by other means) any resource messages. To identify the IT security incident, document as much information as possible. Write down as many details as possible, notes should include date and time. Depending on the system, use the Help Desk, IT Service Desk, or other operational support system to report and document the events or incident.

The email for the IT Service Desk is ITServiceDesk@GSA.GOV. The IT Service Desk will be responsible for initiating incident tickets related to users. IT security staff will also have access to initiate tickets themselves.

Time is critical. Serious incidents with a functional, information, or recovery impact shall be immediately reported upon incident identification to the GSA IT Service Desk. If there is no immediate response during business hours contact Tom Heffron (816-719-0587) or Bo Berlas (202-236-6304). If after normal business hours on-call IR support is available at 202-780-9423. The GSA Incident Response team can also be contacted at gsa-ir@gsa.gov.

Do not delay reporting in order to provide further details (i.e., root cause, vulnerabilities exploited, or mitigation actions taken) as this may result in high risk to the system or enterprise. The GSA OCISO must report such incidents to US-CERT within one-hour.

Confirmed and/or suspected incidents involving the potential loss or compromise of PII in electronic or physical form must be reported IMMEDIATELY to the OCISO via the GSA IT Service Desk. The OCISO will determine when it is appropriate to report incidents to the GSA SAOP. The OCISO will also determine external reporting to the US-CERT, OIG, and U.S. Congress. Reporting will be completed IAW this guide and the US-CERT Federal Incident Notification Guidelines.

3.1.2 Incident Reporting for Externally Hosted Information Systems

The incident reporting form identified in [Appendix B](#) of this guide shall be utilized for incident reporting for all external GSA information systems not integrated with GSA's ServiceNow ticketing system. Further, the form may be utilized in cases of technical difficulty involving

ServiceNow, if necessary. Regardless of incident reporting method, the incident report must be complete and, at a minimum, include the following:

- Reporter's Contact information section (located on page 2 of the form). The Point of Contact (POC) for the incident should clearly identify Name, Email Address, and Telephone Number.
- Provide the date and time the incident occurred and a summary of what happened. Be as precise and as informative as possible. The more information provided, the better the chance of recovery from the incident and prevention in the future.
- Fill in other required information on page 3 of the form. The POC MUST indicate if the incident affects PII.

IMPORTANT: If the information is sensitive (IP address, access information such as an account login and password) do not include it in the form. Sensitive information should not be publicly viewed or transmitted via unencrypted email. A statement should be included that the requested information is sensitive and will be provided in person or via a secured method.

Submit the completed incident report to the GSA IT Service Desk at itservicedesk@gsa.gov and cc the GSA Incident Response Team at gsa-ir@gsa.gov.

It is extremely important to use good judgment, as well as comply with GSA policy regarding sensitivity, when sending ANY information detailing an IT incident electronically.

Confirmed and/or suspected incidents involving the potential loss or compromise of PII in electronic or physical form must be reported IMMEDIATELY reported to the OCISO via the GSA IT Service Desk. The OCISO will determine when it is appropriate to report incidents to the GSA SAOP. The OCISO will also determine external reporting to the US-CERT, OIG, and U.S. Congress IAW this guide and the US-CERT Federal Incident Notification Guidelines.

3.1.3 Incident Reporting for Vendor Identified Incidents (Including GSA Leases)

Incident reporting for vendor identified incidents, including GSA leases, is generally the same as for reporting externally hosted information systems as outlined in Section 3.1.2. The incident reporting form identified in [Appendix B](#) of this guide shall be utilized for incident reporting for vendor identified incidents. However, in addition to submitting the report to the GSA IT Service Desk at itservicedesk@gsa.gov with a cc the GSA Incident Response Team at gsa-ir@gsa.gov, **the report must also be submitted to the Contracting Officer.**

3.2 OCISO's Incident Reporting Responsibilities

The OCISO is responsible for all communications regarding the incident with US-CERT and other external United States Agencies and Departments. The OCISO will notify and coordinate as necessary with other GSA officials. The OCISO submits the GSA Cyber Incident Reporting information to US-CERT and to the OIG, as necessary. Some potentially sensitive or Privacy Act protected information related to the individuals reporting, involved or affected by an incident may be redacted from communications or reports as a precaution. Such information is available by request from US-CERT or the OIG, as necessary.

3.3 OCISO's Threat Awareness Program

It is becoming more likely that adversaries may successfully breach or compromise organizational information systems, because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT). One of the best techniques to address this concern is for organizations to share threat information. This can include sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced and mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives) or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection or less sensitive and freely shared.

The OCISO is responsible for maintaining a threat awareness program that monitors threat intelligence for actionable information and shares this information with relevant system owners, US-CERT, and other government agencies as needed. US-CERT coordinates communication of threat intelligence information between GSA and other Federal agencies. In addition, the OCISO has a program for daily monitoring of network traffic for evidence of data exfiltration. Semi-annual testing is conducting of this data exfiltration review capability.

4 Incident Response Process

GSA is a large, complex and dynamic environment with many IT Services, supplied by various organizational units. For Incident Handling to be effective there must be a common process that is applied across all systems. Some IT systems are strictly local while others are regional or enterprise-wide. To address this GSA uses security roles that are common across all systems (ISSO, ISSM and OCISO) to ensure accountability and authority in handling security incidents. Refer to the [IT Security Procedural Guide CIO-IT Security 18-90](#), "Information Security Program Plan," for common control implementation statements for the [NIST SP 800-53](#) security controls, including the IR controls. The Information Security Program Plan identifies the GSA implementation statements for all common controls and the GSA portion of Hybrid controls for GSA information systems.

Incident response begins as soon as events are suspected of being a *security incident*. It starts with the person or people who first identify and report the events as potential security problems – the "first responder(s)". An important responsibility for people who first suspect a security incident is to protect the system, evidence and the record of events from both malicious and accidental changes until a Tier 2 or Tier 3 Incident Handling Team arrives. Once the Incident Handling Team is actively engaged the "first responder" should provide on-site support as needed.

Tier 1

Who: Local staff, Helpdesk/IT Service Desk, ISSO

What: Determine if it is an incident.

Tier 2

Who: Enterprise Staff, ISSO, ISSM

What: Respond or Escalate to OCISO

Tier 3

Who: OCISO, Enterprise Staff

What: Report, Investigate, Respond

In GSA, as in most agencies, Incident Handling is done on a “Tiered” basis. There are 3 tiers. Tier 1 involves the initial determination whether there has been a security incident and/or further investigation is necessary. This is done by the on-site person reporting abnormal or suspicious system activity to the ISSO. A ticket in the GSA IT Service Desk should be opened by this point. If a Help Desk or Service Desk is the origin of the response, tickets should be flagged with a break/fix or emergency identifier to ensure a timely attention.

The ISSO is responsible for ensuring the security of the systems under his/her control. This includes the process of identifying, reporting, and responding to security events and incidents. As events are identified as security related, they should be either addressed immediately in documented processes or the ISSO should be notified. The system staff under direction of the ISSO will determine if suspicious security events indicate a security incident and require further investigation. In the absence of clear guidance, the ISSO should err on the side of escalation.

Criteria indicating a need for escalation include the following:

- Is there loss of GSA information, especially sensitive information or PII?
- Has the integrity of GSA information been compromised? Is there damage to GSA equipment?
- Could the event be the result of a failure of some security control?
- Is there evidence that several security events are related?
- Have related events been occurring over a period of time or in various locations?
- Is there evidence that more than one system or device was involved or affected by the security event(s)?
- Could further investigation prevent future security events of this kind?

If the ISSO determines that the event needs further investigation or should be classified as an incident, it is escalated to Tier 2. Tier 2 is handled by the ISSO, ISSM and the Enterprise technology team that manages the systems involved¹³. If the event is deemed to be a serious or potentially serious, it is also escalated to Tier 3. Incidents with a functional, information, or recovery impact must be reported immediately to Tier 3.

Tier 2 response to a **non-serious incident** is to handle the incident directly without support from Tier 3 staff or the OCISO¹⁴. Tier 2 staff must document the incident and response, report the incident to OCISO via the ISSM as described in the previous section, remediate the problem and restore the system before closing the ticket. Examples of non-serious incidents could include an improper usage incident that does not involve sensitive information or other systems.

However, if this is a **serious incident**, then it will be escalated to Tier 3 (GSA Incident Response Team staff designated by the OCISO) for a coordinated response. The ISSM and OCISO will make the escalation decision based on various factors including but not limited to the following:

¹³ Not all systems have Enterprise support. In cases where there is no Enterprise support service or management, the incident should immediately be escalated to Tier 3 for resolution with assistance of the OCISO staff.

¹⁴ Notification and reporting requirements must be followed regardless of the escalation that occurs in the three tiered incident handling process.

- Important or significant incidents;
- Incidents with legal or political implications;
- Incidents that involve privacy information, classified information or other federally protected information;
- Incidents that involve other federal agencies;
- Incidents that require security experience or resources not otherwise available.

Response to serious incidents by Tier 3 usually entails assistance from Tier 1 and Tier 2 staff. Tier 2 staff along with Tier 1, should document information or evidence about the incident and the system, including users, accounts, passwords, applications, etc. that would be helpful for a Tier 3 investigation. In cases where legal action is a possibility, the case must be handled using chain of custody rules and documentation. In such cases, the OCISO should be immediately contacted for guidance.

Response staff must also ensure that any affected system is isolated. For example, it may be disconnected from the network by disconnecting the network cable. **However, the system itself should not be used, logged into, unplugged, rebooted or in any way changed without coordination with the Tier 3 Security Engineering Division (ISE) incident investigator.** Tier 3 staff will investigate root cause(s) and assess any damage sustained, as well as identify measures to mitigate future vulnerability to similar incidents. Once Tier 3 gives permission, Tier 2 will restore the system and return it to service.

Figure 2 is a swim chart of the 3 Tiers and the associated decision points.

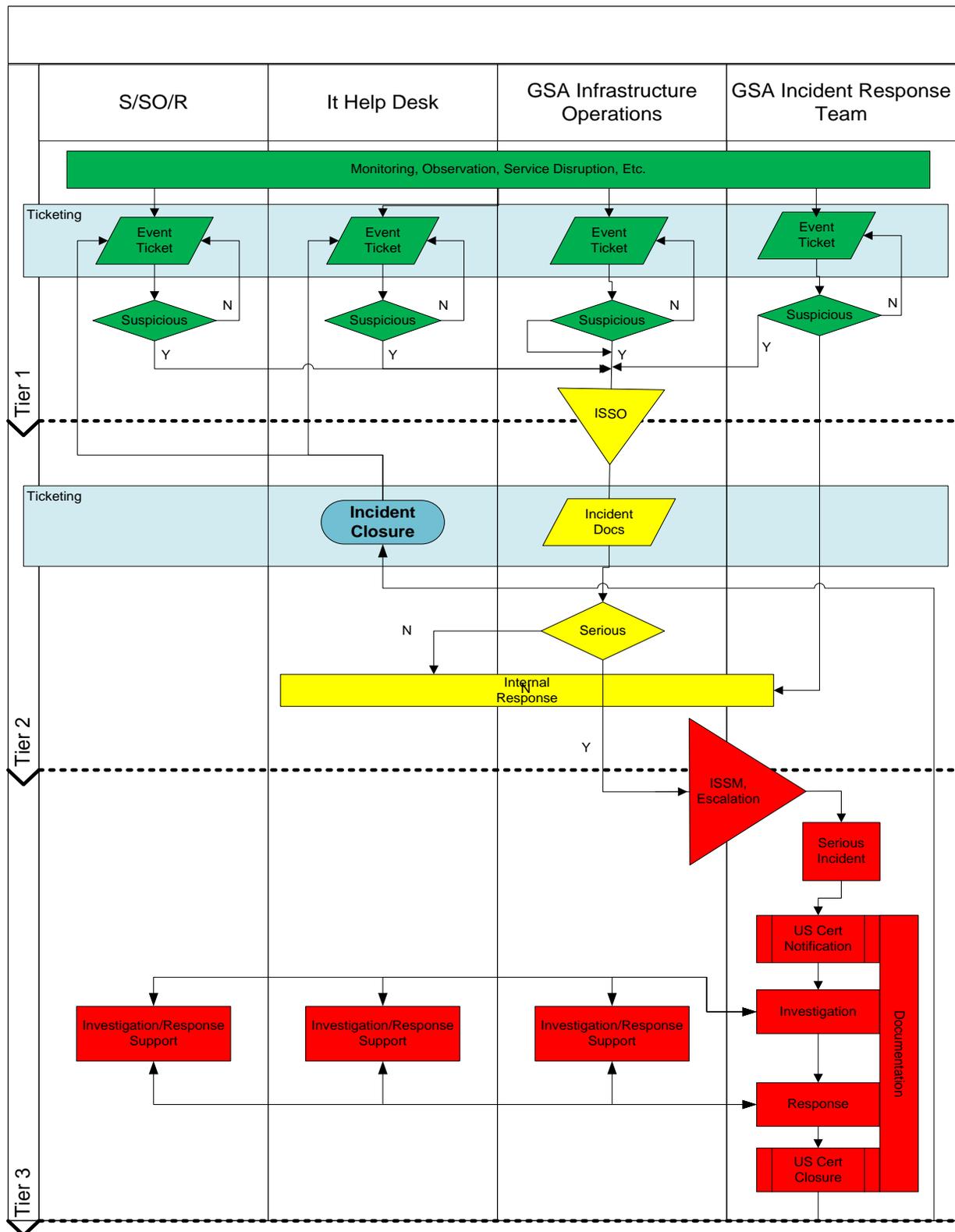


Figure 2: Incident Handling, Response, and Reporting Swimchart

4.1 Tier 1: Initial Determination and Reporting

This section outlines the Tier 1 response tasks, objectives, responsibilities, and incident types.

4.1.1 Tier 1 Response Tasks

The Tier 1 response tasks are to:

- 1) Observe a suspicious event or an actual incident.
- 2) Open a new IT security incident ticket in ServiceNow.
- 3) Serve as an eyewitness to Incident Handling Teams as needed.
- 4) Stabilize the system using techniques appropriate to the type of incident.

4.1.1.1 Who

The first responders to incidents are those who notice and report any events suggestive of a security incident. This includes end users, Help Desk or IT Services staff, system staff, the ISSO, or anyone else who is present. The first responders should report the events and suspicious activity to the GSA IT Service Desk for documentation in ServiceNow, the GSA ticketing system, and fill out the GSA Cyber Incident Response Form for the ISSO to submit.

The ISSO is responsible for coordinating a Tier 1 response. The ISSO must collect enough information from the first responders to accurately make a decision. In cases where the ISSO is not available, the GSA IT Service Desk should know the Tier 2 and Tier 3 escalation procedures and POCs for further action.

4.1.1.2 Objective

The Tier 1 response objective is to sort events into priority, alert the Tier 2 team of the suspected incident, provide enough information for the Tier 2 to determine the seriousness of the incident, and establish the time frame for any required actions.

4.1.1.3 Responsibilities

The Tier 1 response team will notify the ISSO that one or more events are suspicious and may be a part of a security incident. The Tier 1 team accurately report events through ServiceNow, the GSA Ticketing System. The Tier 2 team observes and records unusual behavior of systems, software or people who may be involved, and categorizes the Incident Type or Types.

4.1.1.4 Incident Types

The response required depends upon the type of incident. Table 3 describes the incident types included in the GSA Cyber Incident Reporting Form:

Table 3: Incident Types

Incident Type	Description
Denial of Service	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Improper Usage	A person violates acceptable computing use policies.
Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Incident Type	Description
US-Cert Keylogger	Entered by the ISE only. Please enter all suspected keyloggers as "Malicious Code", if the alert did not come from the US Cert office. This category includes any activity of logging the keys pressed via a hardware device or software application.
Lost Device	Any GSA furnished equipment (GFE) not in the possession of its assigned person
Malicious Code [Not PII]	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.
Phishing Attempt [No exfiltration of data]	The activity of defrauding an online account holder of financial information by posing as a legitimate company, typically by sending an e-mail that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.
PII Incident [Not Lost/Stolen]	Confirmed and/or suspected incidents involving the potential loss or compromise of Personally Identifiable Information (PII) in electronic or physical form.
Reconnaissance Activities	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit.
Stolen Device	Any GSA furnished equipment (GFE) in the possession of an unauthorized person
Unauthorized Access [Not PII]	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource

4.2 Tier 2: Follow-up and Restoration

This section outlines the Tier 2 response tasks, objectives, and responsibilities.

4.2.1 Tier 2 Response Tasks

The Tier 2 response tasks are to:

- 1) Determine if the incident represents a serious threat.
- 2) Verify OCISO notification and reporting.
- 3) Coordinate with Tier 1 (and sometimes Tier 3) staff to handle the incident.
- 4) Collect the "live-state" data from suspect machines using incident response software
See [Appendix C](#).
- 5) Isolate all systems that appear to be involved in Denial of Service, Malicious Code and Unauthorized Use incidents.
- 6) Work with Tier 3 staff, when necessary, to analyze the integrity of the affected systems.
- 7) Remediate vulnerabilities and restore integrity of system.
- 8) Return the system to service.

4.2.1.1 Who

The Tier 2 responders are GSA IT Services staff who are given responsibility to respond to and recover from security incidents in coordination with the ISSO and ISSM. Tier 2 staff should have excellent knowledge of the GSA enterprise network and the experience and judgment to gauge the seriousness of a potential threat to other systems in the environment.

4.2.1.2 Objectives

The Tier 2 response objective is to ensure the course of the response to each incident is carried out to completion. The Tier 2 responders establish a remedial action, ensure a system's return to service, ensure incident reporting is complete, and ensure the incident is documented until closure.

4.2.1.3 Responsibilities

Tier 2 responders must facilitate quick and effective response and recovery. Tier 2 responders make the call regarding the need for isolation of the system from the rest of the network, based on the seriousness of the incident and the criticality of the system.

When an incident has been escalated to Tier 3, Tier 2 responders must provide the Tier 3 staff access to evidence wherever it is in the enterprise. Tier 2 responders must either provide the raw data requested by Tier 3 Incident Handling Team or access to the systems so that relevant evidence may be collected. Tier 2 responders should be prepared to run commands on victim systems and provide the results to the Tier 3 team. Tier 2 responders should also ensure the systems and other evidence that may be used in the investigation are protected from inadvertent or malicious damage. In serious incidents, a compromised system should be locked up or attended until Tier 3 staff are present to take custody of the evidence.

Once the evidence has been collected and a remediation plan has been agreed upon, Tier 2 staff carry out the remediation, test the system to ensure it is clean and hardened, and return the victim system(s) to service.

4.3 Tier 3: Investigation and Counteraction

This section outlines the Tier 3 response tasks, objectives, responsibilities, and forensic tools used by the Tier 3 responders.

4.3.1 Tier 3 Response Tasks

The Tier 3 response tasks are to:

- (1) Direct collection of data for investigation and analysis.
- (2) Provide technical support and leadership for the Response Team.
- (3) Conduct detailed analysis of all evidence.
- (4) Prepare a report that provides detailed description of the incident including:
 - a) damage to Confidentiality, Integrity and Availability of data;
 - b) summary of attackers' methodology;
 - c) vulnerabilities exploited;
 - d) remedial actions; and
 - e) proposed preventive actions.

4.3.1.1 Who

The Tier 3 response to security incidents is handled by the GSA Incident Response Team in the OCISO's Security Engineering Division. The Tier 3 team is trained in Security Incident Response and Forensic Investigation.

4.3.1.2 Objectives

Tier 3 investigation seeks to understand the nature, course and effect of the security incident. The specific level of detail should be set for each incident based on guidance from the OCISO. Tier 3 responses should, at a minimum, result in an assessment of incident prevention and the adequacy of existing security controls.

4.3.1.3 Responsibilities

The Tier 3 team provides expert guidance to Tier 2 responders and conducts the investigation of the incident and its consequences. Tier 3 staff approves the remedial action and return to service (in consultation with the OCISO). Tier 3 staff must secure evidence so that a defensible investigation is possible. Finally, Tier 3 staff reports the investigative findings to the OCISO. The Tier 3 response team is also identifies preventative security measure to protect the enterprise against future security incidents.

4.3.1.4 Tools

Forensic tools for incident response are dynamically evolving. See [Appendix C](#) for a listing of potential tools for live state investigation and detailed forensic analysis.

[GSA Online University](#) has a subscription to Books24x7 available to GSA employees and contractors, which includes books that identify best practices in incident response tools and processes. As of the drafting of this document, the following books are available at no cost:

- Luttgens, Jason T., and Matthew Pepe, *“Incident Response & Computer Forensics”*, Third Edition, McGraw-Hill/Osborne © 2014.
- Johnson III, Leighton R., *“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”*, Syngress Publishing © 2014.
- McCarthy, N. K., *“Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk”*, McGraw-Hill/Osborne © 2012.

In addition, the follow book contains practical commands, scripts, and processes for responding to an incident (but is not available via Books24x7):

- Murdoch, Don, *“Blue Team Handbook: Incident Response Edition”*, Version 2, VMLT © 2014.

In some cases, GSA OCISO, forensic investigators use various tools in the collection and analysis of evidence. If the incident includes a compromise to a system, and the analysis of live-state evidence does not explain or characterize adequately, the capture of disk images may be called for using bit-for-bit storage imaging software. The analysis of these images may use tools such as Encase Examiner, FTK or various open source tools.

4.4 Incident Response Plan Testing and Exercises

Incident Response Plan testing validates the content of IR plans and improves effectiveness of incident response capabilities to prepare for, respond to, manage, and recover from adverse events that may affect GSA information systems. Testing activities focus on likely scenarios informed by the threats to and the vulnerabilities in the GSA IT environment.

Consistent with NIST SP 800-53 control IR-3 (see Section 6 for details), FIPS-199 Moderate and High impact systems must implement annual IR testing and exercises in accordance with this guide and NIST SP 800-61. The activity can be implemented separately or integrated with the system's annual contingency plan test as described under control CP-4, Contingency Plan Testing and Exercises, in NIST SP 800-53. The activities are closely related. [NIST SP 800-84](#), "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," provides additional guidance on how to conduct these tests and exercises.

Enterprise-wide controls identified in this document, which include programmatic controls and processes for OCISO response to serious incidents, are tested biannually in accordance with NIST SP 800-61 and NIST SP 800-84. Results of the annual test are documented in an IR test report. The IT Security webpage contains a general [Information System Contingency Plan Test Report Template](#) which can be used for incident response test reports as well. In addition, the IART conducts annual breach response testing.

4.5 Incident Response Plan Training

Personnel with Incident Response responsibilities generally require broader knowledge than most IT staff members as they work with many facets of IT. Personnel with Incident Response responsibilities require sufficient training to maintain networks, systems, and applications in accordance with the GSA security standards.

GSA information systems, including vendor owned / operated systems on behalf of GSA, shall provide initial training to staff in their incident reporting and response responsibilities in agreement with this document when required by information system changes, and annually thereafter consistent with control requirements.

OCISO also provides training to members of the GSA Incident Response Team within 60 days of joining and annually thereafter. Follow-on annual training is integrated with biannual OCISO testing of the GSA Incident Response Plan in agreement with GSA IT Security Procedural Guide 01-02, *Incident Response* (this guide). This training ensures that team members are able to respond to and manage adverse situations involving IT, using the established procedures documented in this document and supporting standard operating procedures (SOP). Training focuses on OCISO processes for responding to incidents and using GSA enterprise IT and IT security tools. Incident response training relating to process focuses on the following activities:

- Verifying the source
- Verifying the incident
- Notifying responsible parties, including GSA management, US-CERT, OIG, and other law enforcement as necessary
- Forming incident handling team

- Gathering evidence
- Containing, eradicating and recovering from the incident
- Performing follow-up activities after the incident is resolved

Members of the GSA Incident Response Team must understand how to use the tools of incident response, such as computer forensics software identified in [Appendix C](#). Refer to NIST SP 800-84, for more specific guidance in developing, conducting, and evaluating IR training activities. In addition, the IART leads annual breach response training.

4.6 Incident Response for Phishing Attempts

All users are responsible for reporting phishing attempts to the IT Service Desk. All confirmed/suspected phishing incidents are reported to the IT Service Desk. The IT Service Desk is responsible for initiating, performing initial triage and collecting available incidents indicators. All confirmed or suspected phishing incidents are routed to the GSA Incident Response Team as a SEC-type (security) ticket with the details of the phishing attempt.

4.6.1 Differences between Phishing Attempt, Spam, and Social Engineering

The following definition highlights the differences between a phishing attempt, spam, and social engineering:

- **Phishing Attempt:** Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (Source: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms)
- **Spam:** The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages (Source: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms)
- **Social Engineering** - A general term for attackers trying to trick people into revealing sensitive information or performing certain actions. This may be via a phone call, by email, or in person. (Source: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms)

[NIST IR 7298 Revision 2](#), “Glossary of Key Information Security Terms” is the source for the terminology in this section.

4.6.2 Identification Standards for Reporting Phishing Attempts to US-CERT

In accordance with updated US-CERT guidance, the GSA Incident Response Team will generally report only successful attempts to US-CERT that have a potential impact to confidentiality, integrity, or availability, as follows:

- Phishing attempts where ENT domain credential or credentials to other GSA systems are used to gain unauthorized access; or results in malicious code being successfully executed on a GSA server or workstation will be reported with the appropriate functional, information, and/or recoverability impact classification.
- If sensitive information is revealed in spear phishing attempt via email or other means, it will also be reported as an incident with the appropriate information and recoverability impact classification.

- Per US-CERT guidance, other phishing attempts will not be reported as an incident, but submitted separately to phishing-report@us-cert.gov for US-CERT to add the indicators to its detection systems, but not count these as incidents from their perspective. However, the GSA Incident Response Team may choose to voluntarily report phishing attempts to US-CERT at its discretion, such as those in which GSA appears to have been targeted.

Scam (e.g., prescription drugs, 419 scams) and spam emails are not reported, but sent to the Email Team for blocking the sender via a request through the IT Service Desk. Users are directed to “Report Spam” through Google. The action automatically removes all like messages from the user's inbox (if any) and trains Google detection capabilities.

4.6.3 User Communications

Users are instructed to report all suspected or confirmed phishing attempts to the IT Service Desk. To assist in users identifying phishing attacks, users should be referred to US-CERT's Security Tips on Recognizing and Avoiding Email Scams and Avoiding Social Engineering and Phishing Attacks for additional techniques and recommendations. As part of the GSA Incident Response Team's incident remediation, users will be directed to “Report Phishing” through Google. The action automatically removes all like messages from the user's inbox (if any) and trains Google detection capabilities.

The IT Service Desk maintains a Knowledge Base (KB) article that identifies how analysts should handle phishing attempts, as noted below:

- If spam, the email is forwarded to the Email Team for blocking
- If phishing:
 - Request information of the phishing attempt from the user, including whether email contained links or attachments and whether they clicked the link or downloaded the attachment (as applicable)
 - Obtain a copy of the email headers from the user
 - Instruct users not to delete the email until directed by the GSA Incident Response Team
 - Create a security-type (SEC) ticket in ServiceNow that will be assigned to the GSA Incident Response Team for response actions.

In addition, users are reminded about phishing attempts in several ways:

- Regular reminders to all GSA employees and contractors via email.
- In GSA's annual Security Awareness, users are presented with phishing definitions, concepts, and instructions.
- OCISO's Security Operations Division (ISO) conducts annual phishing exercises; users that clicked are directed to a training page.
- In general, when the GSA Incident Response Team encounters users that did not report phishing incidents properly, feedback is provided.

4.6.4 Response Process for GSA Incident Response Team

This section contains a high-level overview of the steps that the GSA Incident Response Team conducts when a phishing attempt is identified. User notifications via IT Service Desk and

corresponding ServiceNow tickets are the primary means of interacting with the GSA Incident Response Team to report a phishing attempt. However, the GSA Incident Response Team also reviews the following sources regularly:

- itsecurity@gsa.gov inbox
- Emails sent directly to the GSA Incident Response Team via gsa-ir@gsa.gov
- Email sent directly to a GSA Incident Response Team member

4.6.4.1 Step 1 - Analysis - Obtain a Copy of the Headers and Body

The GSA Incident Response Team will obtain copy of headers and body (if we do not already have a copy).

4.6.4.2 Step 2 - Analysis - Verify the Phishing Incident

The GSA Incident Response Team will review characteristics of the email for reputation and content to classify the message as a phishing attempt, spam / scam email, or a legitimate email.

4.6.4.3 Step 3 - Containment - Initiate Domain / IP / Email Blocks, Binary Bans

Once an email is confirmed to be a phishing attempt, the GSA Incident Response Team will initiate domain, IP, and email-based blocks based on the attributes identified when classifying the message. In addition, any binaries related to the phishing attempt will be banned in the GSA whitelisting tool (Bit9).

4.6.4.4 Step 4 - Containment - Identify Impacted Users

Upon initiation of necessary blocks outlined in Section 4.6.4.3 Step 3 (i.e., binary, URL, IP, sender/subject, etc.), the GSA Incident Response Team will identify work with the Email team to identify all impacted users receiving the phishing message or a derivation of the phishing message. Phishing emails are generally sent in batches which may include some common indicators (e.g., sender, subject, email text, links, attachments, etc.).

4.6.4.5 Step 5 – Identify Vulnerable Users

Vulnerable users (i.e., users who clicked or brought down and executed an attachment) can be identified at multiple levels using GSA's security fabric. A binary analysis is performed via Bit9. The analysis is looking for the presence and execution of malicious binaries. The Security Incident and Event Management (SIEM) analysis is performed to determine successful connections from the GSA network (including VPN) to malicious IP addresses or websites. The SIEM analysis detects the development of custom FireEye HX Indicators of Compromise (IOCs) with either targeted or enterprise sweeps.

4.6.4.6 Step 6 - Eradication/Recovery - Additional Mitigation Actions (if Needed)

For instances in which the user provided credentials to a phishing website or executed a malicious attachment, additional mitigation actions are needed, including credential resets;

malware mitigation on the affected device(s); forensic analysis; and/or reimaging of the affected device.

4.6.4.7 Step 7 - Post Incident Activity - Enter into ServiceNow and Report to US-CERT

Information related to the incident must be entered into ServiceNow and reported to US-CERT IAW reporting guidelines.

4.6.4.8 Step 8 - Post Incident Activity - Lessons Learned (as Necessary)

For serious incidents or those in which problems in response were identified; conduct a Lessons Learned meeting reviewing the incident to identify necessary improvements including people, process, and technology.

4.7 Incident Response for Lost / Stolen Devices, PIV Cards, or Tokens

GSA's IT Security Policy requires that all incidents be reported to the GSA IT Service Desk, including, but not limited to, lost or stolen mobile devices, PIV cards, or Short-name Account (SNA) tokens. Users have the following additional reporting responsibilities for these incidents:

- Users must also report to DHS's Federal Protective Services all lost or stolen mobile devices (including those that occur outside federal facilities) via the appropriate Regional Hotline, as directed by the appropriate ISSO or GSA IT Service Desk.
- Mobile devices lost or stolen outside of GSA Federal facilities are also required to be reported to local police.
- Lost PIV cards must be reported to the Regional Office of Mission Assurance (OMA) office, as directed by the appropriate ISSO or GSA IT Service Desk.

US-CERT has requested that agencies no longer report to them the following incidents:

- Lost or stolen mobile devices that are encrypted.
- Simple loss or theft of PIV card without any attempts for unauthorized usage.

Once the user reports a lost or stolen mobile device, a task in ServiceNow is generated to remotely wipe the device. RISSOs are responsible for handling these incidents and escalating any unencrypted losses or unauthorized access to the GSA Incident Response Team.

At the request of the OIG, the GSA Incident Response Team will report any stolen devices or PIV cards to them upon detection (see Section 5.3.4 for details).

4.8 Incident Response for PII

PII incidents generally follow the same process and mitigation activities but include escalation within 1 hour to the IART as soon as potential PII is found to be at risk, in accordance with US-CERT guidelines. Details are in [CIO 9297.2C](#).

For Major Incidents involving PII, see above.

PII incidents must be confirmed and evidence of notification provided, as necessary, within ninety (90) days of escalation to the IART, absent certain exigent circumstances, for example:

involvement of internal or external law enforcement entities; large numbers of individuals or voluminous amounts of information at risk; large numbers of address validations and/or notifications required; etc. The SAOP and Full Response Team determine the timeline for incidents under their respective purviews.

5 How Does the OCISO Respond to Serious Incidents?

5.1 Step 1: Verify the Source

Determine whether the source of the initial IT incident information is an internal staff member or outside of GSA (e.g., contractor or former employee).

5.2 Step 2: Verify the Incident

Verify the security incident directly, if possible. Ensure that the IT incident is not a harmless misunderstanding or hoax. Beware of false alarms and other activities that may resemble something serious.

5.3 Step 3: Notify Other Parties

5.3.1 US-CERT

The OCISO provides the United States Computer Emergency Readiness Team (US-CERT) with incident reports for all GSA incidents as defined in Section 3 of this guide.

5.3.2 Other Organizations

Determine if the incident affects other services or organizations. If so, establish a contact list for notification. This step will also aid the OCISO in determining whether legal counsel or law enforcement involvement is warranted.

5.3.3 GSA Management

The OCISO is responsible for notifying agency management including the Authorizing Official (AO), GSA CIO, and the GSA Administrator about significant incidents. The GSA SAOP will be notified of all incidents that involve PII. All incidents involving data breaches which could result in identity theft are coordinated through the OCISO and the GSA Initial Agency Response Team using GSA Order 9297.2 per OMB Memorandum M-17-12.

Note: The required controls to protect government-furnished mobile devices (i.e. full disk encryption, automatic wipes after failed access attempts) are sufficient such to prevent unauthorized access to these devices. Therefore, these incidents will not require reporting to the GSA Initial Agency Response Team, even if PII is reported to be on the device. Reports will be sent to external organizations as identified in this section.

5.3.4 GSA Inspector General

After an incident is reported to the OCISO, the following criteria are used to analyze the incident to determine if it should be reported to the Inspector General (IG).

5.3.4.1 Activities to Report

The OCISO shall promptly notify the OIG of the following types of incidents:

- Potential criminal activity, which includes but is not limited to, computer or software theft, mobile device theft, child pornography, drug dealings, stealing or altering sensitive data, death threats or harassing the public through computer access.
- Improper Usage incidents
- Stolen mobile devices
- Any other incident that is forwarded to US-CERT

The GSA OIG will coordinate further reporting to other law enforcement authorities with jurisdiction. If an incident is determined to be reportable to the OIG, the OCISO will contact the OIG at OIG.CERT.Alert@gsaig.gov. If the OIG takes the investigation, the OCISO will assist the OIG, as needed. If the OIG does not take the investigation, the OCISO will handle the incident utilizing the GSA Incident Handling Procedures.

5.3.4.2 Activities Not to Report

All Denial of Service, Malicious Code, Scans/Probes/Attempted Access incidents, or simple loss of mobile devices and/or laptop computers that do not contain PII. If an incident is determined to be reportable to the IG, the OCISO will communicate this through agreed upon channels.

5.3.5 Reporting Major Incidents to U.S. Congress

FISMA of 2014 requires Federal Departments/Agencies (D/As) to report “major incidents” to the U.S. Congress within seven days of detection. The requirements outlined in M-18-02 are detailed in Section 2.5. Escalation of incidents to the Full Response Team by the GSA Incident Response Team can occur in one of followings ways:

- US-CERT recommends identifying the incident as a major incident in accordance with their analysis as a High (Orange) in the NCISS (see Section 2.4); or,
- More than 100,000 PII records are affected; or,
- At the discretion of the GSA Incident Response Team based on its analysis of the factors included in NCISS (see Section 2.4).

PII incidents escalated to the Full Response Team for major incident determination will be analyzed for both PII factors as well as non-PII factors and, as identified in Section 2.5.

Membership of the Full Response Team is outlined in Section 1.3.

5.3.6 Reporting Incidents to the Office of Mission Assurance’s Insider Threat Program

The OCISO will also notify the Office of Mission Assurance (OMA) upon notification of the GSA Inspector General (as identified in Section 5.3.4), as agreed upon between the GSA Incident Response Team and OMA’s Insider Threat Program. OMA’s Insider Threat Program is outlined in [ADM P 2400.1](#), “Insider Threat Program.” Any changes to this process will be agreed upon by both OMA and the GSA Incident Response Team.

5.3.7 Reporting Incidents to the Contracting Officer

If OCISO identifies that a GSA contractor associate willfully violated a GSA IT security policy, the GSA Incident Response Team will inform the Contracting Officer in addition to the required

reporting to the Office of Inspector General. Other incidents will be reported to the Contracting Officer at the discretion of the GSA Incident Response Team.

5.4 Step 4: Form Incident Handling Team

The OCISO maintains the capability for Tier 3 response to security incidents. The GSA Incident Response Team is empowered to be the *Incident Commanders*, responsible for directing and managing GSA cybersecurity incidents in accordance with [FY 2018 CIO FISMA Metrics](#). Tier 3 may require expertise from managers, technical staff, and security personnel. Tier 3 provides coordination when and if the involvement of legal counsel or law enforcement is necessary (e.g., FBI, GSA OIG). Identified personnel participating on the Incident Handling Team should be notified immediately once an incident has been confirmed. For PII incidents, Tier 3 will provide support to the Initial Agency Response Team or Full Agency Response Team in accordance with GSA Order CIO 9297.2C, "GSA Information Breach Notification Policy". In addition, if the incident is a major incident, Tier 3 will support the Full Response Team, as requested by the Security Engineering Division Director.

The OCISO maintains a contract for 24 x 7 secure operations / incident response support that is available to assist with Tier 3 incident handling. The incident support contractor can be deployed at the discretion of the CISO to assist in incident response activities. The OCISO will put forth a best effort to coordinate the incident response activities with the affected systems' ISSO and ISSM. Additional information regarding this process is available by contacting the OCISO.

5.5 Step 5: Gather Evidence

The Tier 3 staff should develop a plan to collect and analyze evidence needed in the Incident response. Data and other evidence must be gathered and preserved as soon as possible. Evidence gathering generally involves the following activities:

- Question personnel involved as soon as the incident has been verified as factual. Anyone located in the area where the incident occurred is a potential witness to related activity and should also be questioned.
- Collect other forms of evidence (e.g., audit logs and videos from security cameras) that correspond to the date of the IT incident.
- Carefully protect and keep confidential all evidence collected; for example redacting the name(s) of individual(s) who report, are affected or who may have caused an incident from communications and reports.
- Establish and maintain a chain of custody for the evidence.

5.6 Step 6: Contain, Eradicate and Recover from the Incident

The purpose of containing an incident is to limit the spread and impact of an incident. The Tier 3 Incident Handling Team (in conjunction with the Tier 1 and Tier 2 staff) must decide what containment strategy to use based on the type of incident. For some types of incidents, the Incident Handling Team will also need to remove or disable compromised elements of the

system. Finally, the Incident Handling Team will need to restore the system to normal operations in addition to correcting any vulnerability that allowed the incident to occur.

The OCISO will be responsible for monitoring the status of a security incident until the security incident is resolved and normal business operations are safely restored.

5.7 Step 7: Follow-up after the Incident is Resolved

Under the direction of the OCISO, the ISSM must verify that the incident is, in fact, adequately resolved and normal business operations have indeed resumed. With the help of the OCISO, the ISSM of the affected resource will determine what, if any, new preventive measures should be implemented to guard against the recurrence of a similar security incident and to ensure prompt detection and response.

If required, remediation tasks should be entered in the affected resource's Plan of Action and Milestones (POA&M). Follow-up reports should include the original information submitted and any additional information discovered through ongoing investigations. All information related to the incident should be retained for three years. [General Records Schedule \(GRS\) 3.2, Information System Security Records, Transmittal 28](#), specifies that "computer security incident handling, reporting and follow-up records" should be destroyed "3 years after all necessary follow-up actions have been completed."

All relevant security documentation (e.g., the System Security Plan—SSP) should be revised, if necessary.

6 Best Practices

An incident usually starts with ambiguous information that must be interpreted and enhanced to be useful in response. It is important to prepare a methodology to efficiently collect and process the right information to support decision making and support the actions that must follow to contain, remediate and close the incident.

6.1 Key Questions to Ask

This section outlines a series of questions that can help define and refine the information needed to make appropriate decisions.

6.1.1 Is it an incident or a false positive?

Validate information and support it with corroborating evidence. Odd or unexpected behavior of applications may indicate a security problem, but should be supported by other evidence that confirms a violation of security policy. A useful form of corroboration uses existing events to infer the existence of some other piece evidence that must still be gathered. If that piece of evidence is present, the suspicion is supported.

6.1.2 Is the incident still in progress?

Incidents that are in progress must be handled especially carefully and quickly. In certain circumstances the system can be left connected during the investigation. However, this presents both opportunity and danger. Highly valuable data about the intruder and the

security incident can be captured during the live events, particularly if network traffic can be captured and analyzed. On the other hand, there is potential that additional damage can be done while the responders watch. Leaving the system connected should only be done where protection of GSA network and systems can be assured. However, if live incidents can be observed safely, the information gathered may be very useful in protecting the systems from future attacks. In all cases a “Live Response” should be conducted whether the system is isolated or connected. The system should not be powered down or rebooted until the Incident Handling Team has extracted all data needed from the system.

6.1.3 What is its extent of the incident? Does it involve more than one device?

Depending on the seriousness of the incident and the data involved, an incident can be remediated very quickly. However, the responders need to be sure that they understand the scope of the incident. For example, if the incident involves network connections, these connections could be used to involve other systems within GSA networks. The network security staff should be engaged to help identify traffic that might indicate such connections.

6.1.4 Why is it in this particular device and how did it get there?

Determining the source of the incident and the process whereby it reached the victim device is crucial to preventing similar future exploits. GSA has security controls in place that should prevent incidents. The incident is an indicator that some control is not sufficient to protect the system and needs to be reevaluated or reengineered.

7 Live Response Process

Response staff must also ensure that any affected system is isolated; for example, it may be disconnected from the network by disconnecting the network cable. **However, the system itself should not be used, logged into, unplugged, rebooted or in any way changed without coordination with the Tier 3 ISE incident investigator.** The GSA Incident Response Team will evaluate the incident and determine whether to conduct live response.

Most workstations on the GSA network are running Windows 7 and GSA also has many Windows servers. Live response may involve the GSA Incident Response Team executing a local response script or may be done remotely using a tool such as FireEye HX. HX helps GSA detect, respond and contain advanced attacks, such as the APT techniques related to Windows systems. Using HX, security teams can determine whether there has been a compromise, determine how an attacker breached their defenses, and determine what systems are involved. HX identifies signs of attacker activity and detects malware and its behavior.

In addition, live response can be conducted locally for Windows systems using FireEye Memoryze. This tool provides the Incident Response team the ability to acquire and/or analyze memory images and live systems. FireEye Memoryze can include the paging file in its analysis. The GSA Incident Response Team can also retrieve live state information from other platforms, including Unix/Linux systems, using appropriate tools.

8 Summary

An effectively implemented Incident Handling process allows everyone to understand roles and responsibilities that ensure IT security incidents are properly reported, damage is immediately identified and contained, and possible effects are minimized. Failing to report and/or respond to IT security incidents could result in serious adverse consequences for GSA and limit the agency's ability to fulfill its mission.

Every S/SO/R must have a documented incident handling process. It is also important to employ various mechanisms (including, but not limited to, an intrusion detection system) to continuously monitor for possible incidents; see [IT Security Procedural Guide CIO-IT Security-01-08](#), "Audit and Accountability (AU)," for more information. In addition, GSA requires annual assessments of security controls to ensure that they remain effective; see GSA CIO 2100.1, Chapter 3, Policy for Identify Function, Section 4, Risk assessment. Also, GSA employees and contractors must be informed of the incident handling policy and procedures.

Each GSA system must have an ISSO and ISSM who are familiar with the procedures, roles, and responsibilities in this document. Each individual, whether a GSA employee or a contractor, is responsible for reporting any suspicious IT related activity to the GSA IT Service Desk. Serious incidents with a functional, information, or recovery impact shall be immediately reported upon incident identification to the GSA IT Service Desk AND to the GSA Incident Response Team at gsa-ir@gsa.gov or via phone at 202-501-0223 or 202-236-6304.

Confirmed and/or suspected incidents involving the potential loss or compromise of PII in electronic or physical form must be reported IMMEDIATELY reported to the OCISO via the GSA IT Service Desk. The OCISO will determine when it is appropriate to report to the GSA SAOP and when it is appropriate to report externally to the US-CERT, the OIG, and the U.S. Congress IAW this guide and the US-CERT Federal Incident Notification Guidelines.

Where there is a conflict between NIST guidance and GSA guidance, contact the Office of the CISO at gsa-ir@gsa.gov.

Summary of NIST 800-53 IR Controls. [IT Security Procedural Guide CIO-IT Security 18-90](#), "Information Security Program Plan," provides details on IR control parameters, common control implementations, and system specific expectations for GSA. Table 4 provides a mapping of coverage within this procedural guide to NIST 800-53, Revision 4 controls.

Table 4: Mapping of NIST IR Controls to GSA Documents

Control	Control Name	Reference to Control Implementation
IR-1	Incident Response Policy and Procedures	Section 1.2 – Policy Entire Document - Procedures
IR-2	Incident Response Training	Section 4.5
IR-3	Incident Response Testing	Section 4.4
IR-4	Incident Handling	Section 4 (highlighted in Figure 2)
IR-5	Incident Monitoring	Section 4 (use of ServiceNow ticketing)
IR-6	Incident Reporting	Sections 2, 3, and 4
IR-7	Incident Response Assistance	Section 4
IR-8	Incident Response Plan	Entire guide

APPENDIX A - Glossary of Terms

Authorizing Official: The GSA official charged with validating the Authority to Operate and the security controls applied to the system under the Federal Information Security Management Act (FISMA)

Data Breach: The release of sensitive information to an unauthorized party or into an insecure environment, which according to US-CERT guidelines, does not include losses of encrypted mobile devices, or losses of physical information that do not involve a computer

Denial of Service (DoS): An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

Enterprise Staff: GSA staff that support a system and similar systems throughout GSA.

Event: Any observable occurrence in a network or system.

Inappropriate or Improper Usage: A person who violates acceptable use of any network or computer policies.

Identity Theft: Illegal possession and/or usage of Personally Identifiable Information (PII).

Improper Usage: Any activity performed by a person that violates acceptable use of any network or computer policies.

Incident: A violation, suspected violation or imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices.

Incident Handling / Incident Response: The remediation and/or mitigation of violations of security policies and recommended practices.

ISSO: Information Systems Security Officer

ISSM: Information Systems Security Manager

Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Non-serious Incident: An incident that:

- (1) does not require reporting to US-CERT
- (2) does not threaten GSA systems or data and
- (3) can be remediated by local staff without assistance or intervention from the OCISO.

Personally Identifiable Information (PII): PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly

available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g. SSNs, name, DOB, home address, home email).

Privacy Breach: A privacy breach is the actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, and/or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for other-than- an authorized purpose.

RISSO: Regional Information Systems Security Officer

Security Event: An event collected by sensors or reported by observers that may have relevance to security. Events are factual in nature and are separate from any conclusions regarding meaning.

Security Incident: A set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within the enterprise.

Serious Incident: An incident that has confirmed impact to the confidentiality, integrity, or availability of GSA systems and data, has legal, political, or privacy implications, affects other federal agencies, or requires security experience or resources not otherwise available.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other IT resource.

Victim Device: A computer or other system that is the target of or was used in a security incident or a violation of IT security policy.

APPENDIX B – GSA Cyber Incident Reporting Form Instructions

GSA's Incident Reporting Form is available on the [IT Security Forms](#) page.

Instructions

Click on the URL above to locate the Incident Reporting Form.

NOTE: Do not open the document on a computer that has possibly been compromised.

Open the GSA Incident Reporting Form.

Fill out as much of the required information as you know, including the following:

- Reporter's Contact information section (located on page 2 of the form). The Point of Contact (POC) for the incident should clearly identify Name, Email Address, and Telephone Number.
- Provide the date and time the incident occurred and a summary of what happened. Be as precise and as informative as possible. The more information provided, the better the chance of recovery from the incident and prevention in the future.
- Fill in other required information on page 3 of the form. The POC MUST indicate if the incident affects PII.

IMPORTANT: If the information is sensitive (IP address, access information such as an account login and password) do not include it in the form. Sensitive information should not be publicly viewed or transmitted via unencrypted email. A statement should be included that the requested information is sensitive and will be provided in person or via a secured method.

Submit the completed incident report to the GSA Incident Response Team at gsa-ir@gsa.gov.

It is extremely important to use good judgment, as well as comply with GSA policy regarding sensitivity, when sending ANY information detailing an IT incident electronically.

Confirmed and/or suspected incidents involving the potential loss or compromise of PII in electronic or physical form must be reported IMMEDIATELY reported to the OCISO via the GSA IT Service Desk. The OCISO will determine when it is appropriate to report incidents to the GSA SAOP. The OCISO will also determine external reporting to the US-CERT, OIG, and U.S. Congress IAW this guide and the US-CERT Federal Incident Notification Guidelines.

APPENDIX C – Incident Response and Handling Tools

Incident Handling Tools

The GSA Incident Response Team utilizes a number of automated tools and services that are used to assist in incident handling, including:

- *Enterprise Logging Platform* - The SIEM Tool that collects and correlates event log data from network devices across the network including Firewalls, IDP/IPS devices, Web Proxies, and Wireless Access Points.
- *FireEye Endpoint Security (HX series)* - An endpoint-based solution that allows security analysts to conduct detailed investigations to identify and contain Indicators of Compromise (IOC) related to APT malware.
- *Bit9* - Deployed as an application whitelisting solution that identifies executables on GSA workstations/servers in a central repository for investigation into whether malware was executed on a device.
- *Palo Alto Wildfire* - Cloud-based malware detection service which performs static and dynamic analysis of binary executables ingressing the GSA network. Alerts on detection of malware.
- *NetIQ* - Identity Management Tool used for correlating VPN identifiers to users.
- *Cylance* - Cylance provides centralized event collection and reporting for Cylance antivirus software on GSA workstations and servers. It allows security analysts to investigate malware incidents and trends.
- *MaaS360* - The software management tool that GSA uses to deploy and inventory software on workstations and mobile devices.
- *FireEye Managed Defense Portal* - Allows for access to alerts from FireEye regarding threats.
- *CenturyLink Portal* - Allows for access to alerts from the CenturyLink Security Operations Center.
- *FireEye Intelligence* - Allows for access to FireEye (formerly iSIGHT Partners) Vulnerability and Threat Reports.

Forensic Tool Sources

GSA OCISO uses a combination of commercial and open source tools to capture cyber-forensic evidence as part of a Tier 3 investigation. Detailed forensics investigations are also supported by several additional COTS and open source tools, including, but not limited to, the following:

- Mobile Forensics Tools
 - *Katana Forensics Latern* - Allows image acquisition for mobile devices, specializing in iOS.
 - *viaForensics viaExtract* - Provides forensic capabilities for Android devices, including image acquisition.
- General Forensics
 - *FTK Forensic Toolkit* - Provides the ability to conduct detailed forensic investigations on various platforms, such as hard drives, mobile devices, network data, and internet storage.

- *EnCase Forensic Imager* - Provides the ability to acquire forensic images from local disks.
- Live Response Forensics
 - *FireEye Memoryze* - Provides ability to acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis.

Other Tools and Web Site References

- [NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide](#) (particularly Section 3.2 regarding Incident Detection)
- [NIST SP 800-86, Guide to Integrating Forensics Techniques into Incident Response](#)
- [US-CERT, United States Computer Emergency Readiness Team](#)
- [NIST SP 800-88, Revision 1, Guidelines for Media Sanitization](#)