US-CERT Federal Incident Notification Guidelines

This document provides guidance to Federal Government departments and agencies (D/As); state, local, tribal, and territorial government entities; Information Sharing and Analysis Organizations; and foreign, commercial, and private-sector organizations for submitting incident notifications to the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT).

The Federal Information Security Modernization Act of 2014 (FISMA) defines "incident" as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."[1] FISMA requires federal Executive Branch civilian agencies to notify and consult with US-CERT regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source[2]. This includes incidents involving control systems, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs) and other types of industrial measurement and control systems. Reporting by entities other than federal Executive Branch civilian agencies is voluntary.

These guidelines support US-CERT in executing its mission objectives and provide the following benefits:

- Greater quality of information – Alignment with incident reporting and handling guidance from NIST 800-61 Revision 2 to introduce functional, informational, and recoverability impact classifications, allowing US-CERT to better recognize significant incidents.
- Improved information sharing and situational awareness – Establishing a one-hour notification time frame for all incidents to improve US-CERT's ability to understand cybersecurity events affecting the government.
- Faster incident response times – Moving cause analysis to the closing phase of the incident handling process to expedite initial notification.

Notification 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

[1] See 44 U.S.C. § 3552(b)(2). FISMA also uses the terms "security incident" and "information security incident" in place of incident.
[2] See 44 U.S.C. §§ 3553-54. US-CERT serves as the federal incident response center.

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.

Submitting Incident Notifications

The information elements described in steps 1-7 below are required when notifying US-CERT of an incident:

1. Identify the current level of impact on agency functions or services (Functional Impact).
2. Identify the type of information lost, compromised, or corrupted (Information Impact).
3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
4. Identify when the activity was first detected.
5. Identify the number of systems, records, and users impacted.
6. Identify the network location of the observed activity.
7. Identify point of contact information for additional follow-up.

   Important: Please refrain from adding sensitive personally identifiable information (PII) to incident submissions. Any contact information collected will be handled according to the DHS website privacy policy[3].

8. Submit the notification to US-CERT.

The following information should also be included if known at the time of submission:

9. Identify the attack vector(s) that led to the incident.
10. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
11. Provide any mitigation activities undertaken in response to the incident.

Within one hour of receiving the report, the NCCIC/US-CERT will provide the agency with:

- A tracking number for the incident.
- A risk rating based on the NCCIC Cyber Incident Scoring System (NCISS).

Reports may be submitted using the NCCIC/US-CERT Incident Reporting Form; send emails to soc@us-cert.gov or submit reports via Structured Threat Information eXpression (STIX) to auto-submit@us-cert.gov (schema available upon request).

Impact and Severity Assessment

To support the assessment of national-level severity and priority of cyber incidents, including those affecting private-sector entities, the NCCIC will analyze the following incident attributes utilizing the NCISS:

- Functional Impact,

[3] http://www.dhs.gov/privacy-policy

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

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[4].

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)[5] :

- 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): Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of U.S. persons.
- 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.

Major Incidents:

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. Agencies should comply with the criteria set out in the most recent OMB guidance when determining whether an incident should be designated as major.

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

[4] https://www.dni.gov/cyber-threat-framework/lexicon.html
[5]https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf

determines that an incident meets the criteria for High (Orange) on the Cyber Incident Severity Schema, it will suggest that the agency designate that incident as a major incident.

Under Presidential Policy Directive 41 (PPD-41) - United States Cyber Incident Coordination, all major incidents are also considered *significant cyber incidents*, meaning they are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties or public health and safety of the American people. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors as appropriate.

Impact Category Descriptions

The table below defines each impact category description and its associated severity levels. Use the tables below to identify impact levels and incident details.

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.

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.
Information Impact – Describes the type of information lost, compromised, or corrupted.	NO IMPACT – No known data impact.
	SUSPECTED BUT NOT IDENTIFIED – A data

Impact Category	Category Severity Levels
	loss or impact to availability is suspected, but no direct confirmation exists.
	PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII[6]) or personal health information (PHI) was compromised.
	PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information[7], such as protected critical infrastructure information (PCII), 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).
	NOT APPLICABLE – Incident does not require recovery.

[6] As defined in OMB Memorandum M-07-16, “personally identifiable information” refers to “information which can be used to distinguish or trace an individual's identity

[7] 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”

Attack 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 this common taxonomy. Below is a high-level set of attack vectors and descriptions developed from NIST SP 800-61 Revision 2. Federal civilian agencies are to utilize the following attack vectors taxonomy when sending cybersecurity incident notifications to US-CERT.

Attack Vectors Taxonomy

Attack Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack 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/Phishing	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 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 structured query language 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 method does not fit into any other vector	

Incident Attributes

The following incident attribute definitions are taken from the NCISS.

Attribute Category	Attribute Definitions
Location of Observed Activity: Where the observed activity was detected in the network.	LEVEL 0 – UNSUCCESFUL – Existing network defenses repelled all observed activity
	LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
	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.
	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.
	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.
	LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
	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.
	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.
	UNKNOWN – Activity was observed, but the network segment could not be identified.
Actor Characterization	The type of actor(s) involved in the incident (if known). This element is not selected by the reporting entity.

Attribute Category	Attribute Definitions
Cross-Sector Dependency	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.
Potential Impact	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.

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.

These guidelines are effective April 1, 2017. D/As are permitted to continue reporting incidents using the previous guidance until said date.

For questions, please email federal@us-cert.gov.