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 Centers (ISACs); and foreign, commercial, and private sector organizations for submitting incident notifications to the United States Computer Emergency Readiness Team (US-CERT). A computer security incident within the Federal Government is defined by the National Institute of Standards and Technology (NIST) and US-CERT as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

US-CERT acts as the Federal information security incident center for the United States federal government per the Federal Information Security Management Act of 2002 (FISMA).[1] Pursuant to FISMA, each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems (managed by a federal agency, contractor, or other source) that support the operations and assets of the agency.[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 all other entities is voluntary.

These guidelines support US-CERT in executing its mission objectives and enable 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.

These guidelines are effective October 1, 2014, however, all D/As are permitted to continue reporting incidents using the legacy incident reporting category system[3] until September 30, 2015.

---

[1] 44 U.S.C. § 3546.
[2] 44 U.S.C. §§ 3544(b) & (b)(7)(B).
[3] https://www.us-cert.gov/government-users/reporting-requirements

Standard Data Elements

To facilitate effective and consistent incident handling, US-CERT has established a standard set of data elements to collect for each incident report. Incident notifications should include a description of the incident and as much of the following information as possible:

Important: Ensure that any technology used to capture sensitive incident information, including Personally Identifiable Information (PII), is properly secured to preserve confidentiality and integrity.

- Contact information for both the impacted and reporting organizations (unless submitting an anonymous report)
- Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers)
- Date/Time of occurrence, including time zone
- Date/Time of detection and identification, including time zone
- Related indicators (e.g. hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures)
- Threat vectors, if known (see Threat Vector Taxonomy and Cause Analysis flowchart)
- Prioritization factors (i.e. functional impact, information impact, and recoverability)
- Source and Destination Internet Protocol (IP) address, port, and protocol
- Operating System(s) affected
- Mitigating factors (e.g. full disk encryption or two-factor authentication)
- Mitigation actions taken, if applicable
- System Function(s) (e.g. web server, domain controller, or workstation)
- Physical system location(s) (e.g. Washington DC, Los Angeles, CA)
- Sources, methods, or tools used to identify the incident (e.g. Intrusion Detection System or audit log analysis)

Incident Notification

Notifying US-CERT of a computer security incident is mandatory when the confidentiality, integrity, or availability of a Federal Government information system has been confirmed to be compromised. Notification of incidents which have no confirmed functional or information impact such as passive scans, phishing attempts, attempted access, or thwarted exploits may be submitted to US-CERT voluntarily. For voluntary reports, please identify the threat vector and any potential indicators of compromise before notification.

> **Requirement:** US-CERT must be notified of all computer security incidents involving a Federal Government Information system with a confirmed impact to confidentiality, integrity or availability within ***one hour*** of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department.

It is imperative for reporting agencies to adhere to the one-hour timeframe and provide all available information. 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. If the cause of the incident is later identified, the threat vector may be updated in a follow-up report.

Follow the steps below to send an incident notification to US-CERT:

1. Identify functional impact (see Impact Classification table) ***required**
2. Identify information impact (see Impact Classification table) ***required**
3. Identify impact to recoverability (see Impact Classification table) ***required**
4. Identify threat vector (see Cause Analysis flowchart), if possible
5. Provide any mitigation details, if possible
6. Provide contact information and any available incident details ***required**

> **Important:** Please refrain from adding sensitive Personally Identifiable Information [7] (PII) to incident submissions. Any contact information collected will be handled according to the DHS Website Privacy Policy. [4]

7. Submit to US-CERT. Please note that batched reports (multiple, separate incidents in a single submission) will be considered invalid. Reports may be submitted using the US-CERT Incident Reporting Form or by using the contact information available from the US-CERT website.

---

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

Impact Classifications

Please use the table below to identify the impact of the incident. 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 (i.e. all, subset, loss of efficiency) must be defined by the reporting organization.

Note: Please refrain from reporting incidents involving ***non-cyber*** PII exposures or classified data spillage (i.e. unsecured hard copies) to US-CERT. Notify your organization's Privacy Office of all non-cyber incidents involving PII. Contact your Security Office for further guidance on responding to classified data spillage.

Impact Classifications	Impact Description
Functional Impact	**HIGH** – Organization has lost the ability to provide all critical services to all system users.
	MEDIUM – Organization has lost the ability to provide a critical service to a subset of system users.
	LOW – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
	NONE – Organization has experienced no loss in ability to provide all services to all users.
Information Impact	**CLASSIFIED** – The confidentiality of classified information[5] was compromised.
	PROPRIETARY[6] – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	PRIVACY – The confidentiality of personally identifiable information [7] (PII) or personal health information (PHI) was compromised.
	INTEGRITY – The necessary integrity of information was modified without authorization.
	NONE – No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverability	**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.

[5] As defined in CNSSI 4009, "classified information" is "information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."
[6] 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"
[7] 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

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 this common taxonomy.

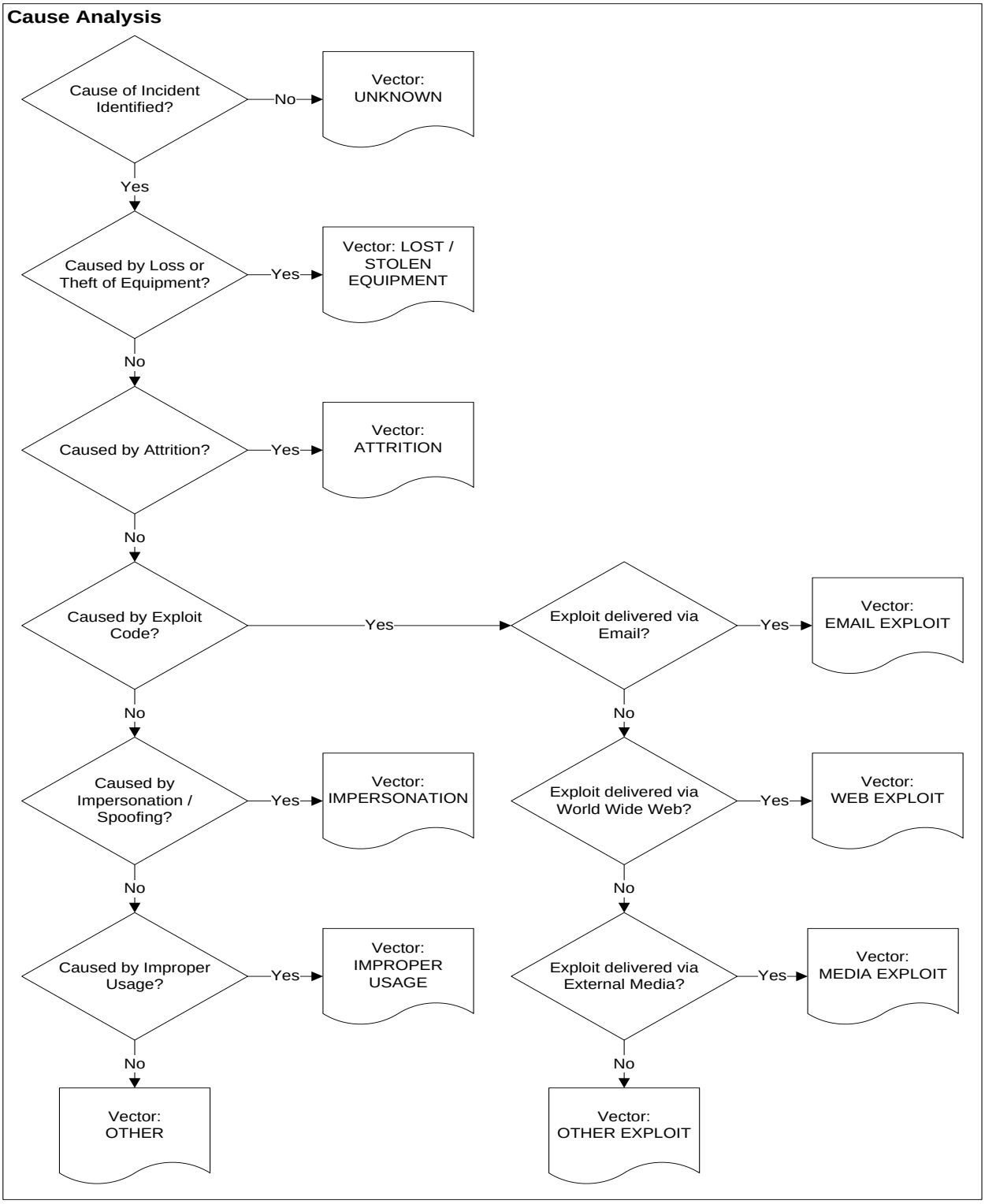
Below is a high-level set of concepts and descriptions developed from guidance in NIST SP 800-61 Revision 2. Federal civilian agencies are to utilize the following threat vectors taxonomy when sending cybersecurity incident notifications to US-CERT.

Threat Vectors 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	

Cause Analysis

Use the decision tree below to assist in identifying the appropriate threat vector:



Incident Examples

Scenario # 1: SQL Injection
An agency reports a successful SQL injection attack on an internal web server. The report confirms that customer data was exfiltrated and an unknown administrator's account credentials were modified. The agency is requesting assistance to contain and recover from the incident.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *Low*
Information Impact: *Privacy, Integrity*
Recoverability: *Extended*
Threat Vector: *Web*

Scenario #2: Anonymous Threat
The organization's physical security team receives a call from an IT manager, reporting that two of her employees just received anonymous threats against the organization's systems. Based on an investigation, the physical security team believes that the threats should be taken seriously and notifies the appropriate internal teams, including the incident response team, of the threats.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *None*
Recoverability: *Not Applicable*
Threat Vector: *Other*

Scenario #3: Peer-to-Peer File Sharing
The organization prohibits the use of peer-to-peer (P2P) file sharing services. The organization's network intrusion detection sensors have signatures enabled that can detect the usage of several popular P2P file sharing services. On a Monday evening, an intrusion detection analyst notices that several file sharing alerts have occurred during the past three hours, all involving the same internal IP address. Upon further investigation, the analyst confirmed that the internal users transmitted unlicensed software during the incident.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *Proprietary*
Recoverability: *Regular*
Threat Vector: *Improper Usage*

Scenario #4: Unknown Wireless Access Point
A wireless intrusion detection system detects an unauthorized wireless access point (WAP) in close vicinity to agency facilities. The WAP's Service Set Identifier is similar to that of an authorized device. Additionally, the unauthorized WAP is causing interference with several authorized WAPs. Physical security is contacted to assist in remediating the issue.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *Low*
Information Impact: *None*
Recoverability: *Supplemented*
Threat Vector: *Impersonation*

Scenario #5: Lost Mobile Device
On 05-15-14 at approximately 9:20am PST, the Help Desk received a report of a missing/lost blackberry smart phone. The appropriate staff has been notified to terminate the phone service. There was no known PII or Controlled Unclassified Information (CUI) information on the device. A "kill-pill" message will be sent to the mobile device that functionally wipes and disables the handset. The device is encrypted with a NIST FIPS 140-2 evaluated and listed encryption. Site does not allow files to be downloaded and locally stored. The device is used for phone/email purposes.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *None*
Recoverability: *Regular*
Threat Vector: *Loss or Theft of Equipment*

Scenario #6: Distributed Denial of Service (DDoS)
A DDoS attack was launched against an agency server causing a firewall failover. The agency experienced a minor outage for approximately 1 hour before the device was fully recovered. Further investigation identified the attack as a DNS amplification attack. There may be additional protocols and ports involved. Agency does not require remote or on-site assistance to recover from the incident.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *Low*
Information Impact: *None*
Recoverability: *Regular*
Threat Vector: *Attrition*

Scenario #7: Data Exfiltration
An OMB MAX account was compromised and used to view 100+ webpages and documents on the OMB MAX server.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *Privacy*
Recoverability: *Regular*
Threat Vector: *Impersonation*

Scenario #8: Malware infection
An agency identified a system that was exposed to malicious content in the form of a Trojan Downloader. The exposure resulted from access to a malicious Internet web site identified and validated through audit log analysis. Enterprise anti-virus solutions detected the malicious content, but failed to prevent infection. The exposure has corrupted the integrity of the data and has impacted the availability of resources. The agency is coordinating with impacted stakeholders to mitigate further risk exposure.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *Low*
Information Impact: *Integrity*
Recoverability: *Regular*
Threat Vector: *Web*

Scenario #9: Phishing
A user responded to a phishing email asking for her web mail login details. The attacker then used the disclosed credentials to access the user's webmail account and send out phishing spam.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *Privacy*
Recoverability: *Regular*
Threat Vector: *Impersonation*

Scenario #10: Man-in-the-Middle
Agency reports successful man-in-the-middle attack on a public wireless network involving the capture of authentication credentials.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *Privacy*
Recoverability: *Regular*
Threat Vector: *Impersonation*

Scenario # 11: Unauthorized Access without Data Breach
During the course of daily scans, an agency's system detects an unknown host on the internal network. After further analysis the agency's computer incident response team identifies that the intruder used obfuscation techniques to breach an agency network. They uncover that the individual did not access agency data due to internal security and access controls. In response the agency updated firewall rules to block the intruder's system.

Correct Impact Classification and Threat Vector selections:
Functional Impact: *None*
Information Impact: *Integrity*
Recoverability: *Regular*
Threat Vector: *Other*