BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-203

16 MARCH 2017

Operations

CYBER INCIDENT HANDLING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/CIO A3CW

Certified by: SAF/CIO A3C/A6C
(Brig Gen Kevin B. Kennedy)

Pages: 28

This instruction implements Air Force Policy Directive (AFPD) 17-2, *Cyberspace Operations*. It describes and provides broad guidance for implementing the Air Force (AF) and Department of Defense (DoD) Cyber Incident Handling Program, the major processes that take place within that program, and the interactions with related U.S. government Defensive Cyberspace Operations (DCO) and DoD Information Networks (DoDIN) Operations activities. It applies to all military and civilian AF personnel, members of the AF Reserve, Air National Guard, DoD contractors, and individuals or activities under legal agreements or obligations with the Department of the AF. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through Major Command (MAJCOM) publications/forms managers to HQ USAF/A6S. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers as directed in the appropriate paragraphs of this Instruction. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the AF Records Information Management System (AFRIMS).

Chapter 1

INTRODUCTION

1.1. Introduction. The AF relies on networked electronic systems to plan and execute its full range of missions around the world. While these systems help us to maintain our military dominance, they also provide our adversaries a means by which to gain an asymmetric advantage via network attack and/or the exploitation of networked systems. AF networks are probed and scanned by domestic and foreign sources thousands of times each day. To counter, negate and mitigate unauthorized activity on its networks, the AF and DoD conduct a wide range of actions collectively known as DCO.

1.1.1. DCO are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities.

1.1.2. This Instruction provides guidance on AF DCO and the conduct of network incident handling. For the purposes of this instruction, DCO and DoDIN Operations refer to day-to-day network monitoring, analysis, detection, and response. They do not refer to missions/actions associated with deliberate mission planning for named defensive operations.

1.1.3. This Instruction also applies to incidents involving systems which are not directly connected to or part of an AF network, e.g., supervisory control and data acquisition (SCADA) systems or information systems that are an integral part of a weapon system and may connect to the DoDIN indirectly through the use of removable media or a wireless connection.

1.1.4. This Instruction does not apply to AF Intelligence Community (IC) and Intelligence, Surveillance, and Reconnaissance systems, networks and assets. These assets fall under the purview of Office of the Director for National Intelligence (ODNI) and HQ USAF/A2.

1.2. Applicability. CJCSM 6510.01B, *Cyber Incident Handling Program*, breaks down adverse actions that occur on DoD networks into ten categories (see Table 1.1). The terms "event" and "incident" are also used to further categorize the actions and to help prioritize the counteractions necessary to detect and prevent future adversary activity of that type.

1.2.1. Event. Committee on National Security Systems (CNSS) Instruction 4009 defines an "event" as any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. Occurrences determined to be Category (CAT) 0, 3, 5, 6, 8, and 9 activity are referred to as events.

1.2.2. Incident. CNSS Instruction 4009 defines an "incident" as an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system (IS); or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. For purposes of this AFI, "information system" includes weapon systems and platform information technology (IT). Occurrences assessed to be CAT 1, 2, 4, and 7 are called incidents. Do not confuse the term "incident" as used in this Instruction with the alternative use of the term to describe network maintenance types of

occurrences (i.e., an "incident" consisting of a customer not being able to access email because his/her account was incorrectly configured by a system administrator).

1.2.3. Incidents Involving Breaches of Personally Identifiable Information (PII). In addition to the procedures specified in this Instruction, incidents which may involve the compromise of PII will also be reported according to the guidelines in paragraph 1.1.2.4 of AFI 33-332, *The Air Force Privacy and Civil Liberties Program*, and Appendix A, Table 1, of Office of the Secretary of Defense (OSD) Memorandum OSD 06227-09, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. **(T-0)**

Table 1.1. Categories of Events (0, 3, 5, 6, 8, and 9) and Incidents (1, 2, 4, and 7).

Category	Description
0	Training and Exercises (Event): Operations performed for training purposes and support to Combatant Command/Service/Agency/Field Activity (CC/S/A/FA) exercises.
1	Root-Level Intrusion (Incident): Privileged access, often referred to as administrative or root access, provides unrestricted access to an IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	User-Level Intrusion (Incident): Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user-level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	Unsuccessful Activity Attempt (Event): Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Note the above CAT 3 explanation does not cover the "run-of-the-mill" virus that is defeated/deleted by AV software. "Run-of-the-mill" viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in the Joint Information Management System (JIMS).
4	Denial of Service (Incident): Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.

5	Non-Compliance Activity (Event): Activity that potentially exposes ISs or networks to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing AF or DoD policy.
6	Reconnaissance (Event): Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	Malicious Logic (Incident): Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS. Unless otherwise directed, only those computers that were infected will be reported as a Category 7 incident.
8	Investigating (Event): Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
9	Explained Anomaly (Event): Suspicious events that, after further investigation, are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as system malfunctions and false alarms. When reporting these events, clearly specify the reason for which it cannot be otherwise categorized.

1.3. DoD DCO and DoDIN Operations Operational Hierarchy. DoD has a three-tiered structure to conduct DCO and DoDIN Operations. NOTE: Do not confuse this with the tier hierarchy used for IT incident management (i.e., network trouble tickets), in which tiers I through III are used with lower numbers corresponding to lower echelons.

1.3.1. Tier One provides DoD-wide DCO and DoDIN Operations operational direction and support to all Combatant Commanders, Services and Agencies (C/S/As). Tier One entities include US Strategic Command (USSTRATCOM) and the US Cyber Command (USCYBERCOM).

1.3.2. Tier Two provides C/S/As DCO and DoDIN Operations direction and support and responds to direction from Tier One. Tier Two includes 24th AF (AFCYBER) with the 624

Operations Center (624 OC) acting as its operational command and control (C2) arm, operating the Cyberspace Command and Control Mission System (C3MS) and providing AF-level command and control (C2) of DCO and DoDIN Operations. It also includes units which operate the Air Force Cyberspace Defense (ACD) weapon system to provide the 624 OC and AF units with incident handling, computer/network forensics analysis, and countermeasures development support. It also includes the 26th Network Operations Squadron (NOS), which operates the AF Intranet Control weapon system and provides support to DCO and DoDIN Operations. Finally, Tier Two also includes assets of 25th Air Force (25AF) (ACC) that provide the ACD weapon system and 624 OC with computer/network foreign threat analysis.

1.3.3. Tier Three provides operational direction and support to local DCO and DoDIN Operations and responds to direction from a designated Tier Two entity. Tier Three includes regionally-focused organizations such as the Network Operations Squadrons (NOS), the MAJCOM Communications Coordination Centers (MCCC)/AFFOR Communications Control Center (ACCC), and local elements such as the base-level Communications Focal Points (CFPs). For purposes of this Instruction, the term MCCC also includes organizational structures established at the discretion of a MAJCOM which perform the same functions as an MCCC.

1.4. Air Force Office of Special Investigations (AFOSI) and other Law Enforcement & Counterintelligence (LE/CI) Agencies. These organizations are not organized within the "tiered" structure. However, they support and operate throughout all tiers. As an LE/CI agency, AFOSI is a critical contributor to effective DCO and DoDIN Operations by providing cyber threat indicators and warnings to commanders; AFOSI establishes and enables attribution and is charged with investigating intrusions and other illegal activity impacting AF information systems and networks. AFOSI's authorities offer access to the civilian/commercial sector not otherwise available to the USAF.

1.5. Other Partners. Other important partners include the Intelligence Community, defense industrial base, and the commercial sector (e.g., anti-virus vendors). These groups have access to resources that can augment and enhance DCO, DoDIN Operations, and incident handling, analysis, and response capabilities.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Directorate of Cyberspace Strategy and Policy (S AF/CIO A6S). Serves as the OPR for Headquarters Air Force development and coordination of policies and guidelines for cyber incident handling.

2.2. Directorate of Security, Special Access Program Oversight and Information Protection (SAF/AAZ).

2.2.1. In coordination with AF/A3, SAF/A6 and SAF/AQ, recommends security protection of new projects/capabilities in accordance with established classification guidance and Department of Defense Instruction (DoDI) O-3600.02, Information Operation (IO) Security Classification Guidance.

2.2.2. Is designated Computer Network Defense Service Provider (CNDSP) Certification Authority (CA) for Special Access Program (SAP) networks and is responsible for coordinating and directing SAP enclave-wide CNDSP activities.

2.3. The AF Inspector General (SAF/IG). SAF/IG provides administrative guidance and oversight to the AFOSI, and provides Executive Agent oversight for the Defense Cyber Crime Center (DC3) as delegated by the SecAF in accordance with DoDD 5505.13e, *DOD Executive Agent (EA) for the Defense Cyber Crime Center (DC3)*.

2.3.1. AFOSI is a Federal Law Enforcement (LE) agency and a member of the Intelligence Community (IC) as executor of the AF's counterintelligence (CI) mission. The AFOSI:

2.3.1.1. Is the sole AF entity with responsibility for conducting felony criminal investigations and counterintelligence activities in and through cyberspace. It is also the sole AF agency responsible for conducting liaison with federal, state, local and foreign nation law enforcement, counterintelligence, and security agencies for matters falling within the AFOSI mission.

2.3.1.2. Provides releasable LE/CI information, threat analysis and indications and warnings (I&W) support to the 624 OC and larger AF DCO and DoDIN Operations community when appropriate.

2.3.1.3. Counters cyber threats by enabling criminal prosecution or conducting counterintelligence activities.

2.3.2. The Defense Cyber Crime Center (DC3). DC3 provides support in intrusion forensics, cyber training for incident response, cyber investigations, digital forensics, and cyber analysis via its Defense Computer Forensics Laboratory and Defense Cyber Investigations Training Academy as well as capabilities in cyber analytics via the DC3 Analytical Group and DoD Defense Industrial Base Collaborative Information Sharing Environment.

2.4. Other Air Staff Offices. Coordinate with SAF/A6S on development of all cyberspace operations-related policy and guidance.

2.5. MAJCOMs, Numbered Air Forces (NAFs), Field Operating Agencies (FOAs) and Direct Reporting Units (DRUs).

2.5.1. **Air Force Space Command (AFSPC).** AFSPC is the lead command for Cyberspace Operations with responsibilities as outlined in AFPD 10-9, Lead Command Designation and Responsibilities For Weapon Systems. In accordance with AFI 17-201, Command and Control for Cyberspace Operations, the Commander, AF Space Command (AFSPC/CC) is responsible for the overall command and control, security and defense of the AF Information Network (AFIN), and for the command, control, implementation, security, operation, maintenance, sustainment, configuration, and defense of the AF Network (AFNET)/AF Network-Secure (AFNET-S). These day-to-day authorities may be delegated.

2.5.1.1. 24 AF / AFCYBER. AFCYBER is the Air Force component to USCYBERCOM. 24 AF/CC, when acting as AFCYBER/CC or when executing missions delegated by AFSPC/CC:

2.5.1.1.1. Issues cyber orders to subordinate 24 AF wings, MAJCOMs, wings, NOSs, and CFPs via the 624 OC and/or the AFSPC Command Center as needed for response to cyber incidents.

2.5.1.1.2. Exercises specific compliance enforcement and directive authority to task the NOSs in response to network events that involve multiple MAJCOMs, affect the preponderance of the AF network, or are time-critical to assure network availability and security. This authority extends to all systems and applications that expose AF networks to a vulnerability or impact operations.

2.5.1.1.3. Provides the Intelligence Community with requirements for priority intelligence and I&W of potential attacks against AF information systems and computer networks.

2.5.1.1.4. Establishes requirements and direction for AF Attack, Sensing and Warning under responsibilities for the National Security Incident Program.

2.5.1.1.5. Engages with the owners of functional systems that are employed and in-use on the AF network, and with appropriate Authorizing Officials (AOs) and their staffs, to ensure that information needed for management of incidents involving those systems is disseminated to levels were it is required to enable appropriate action.

2.5.1.1.6. In his/her role as AF component commander (AFCYBER/CC) to USCYBERCOM, 24 AF/CC ensures AF forces perform the mission and tasks assigned by USCYBERCOM to include the reporting and coordination of network events and incidents.

2.5.1.1.7. 24 AF is designated as the AF CNDSP for AF General Services (GENSER) on NIPRNet and SIPRNet. In this role, 24 AF:

2.5.1.1.7.1. Coordinates and directs AF-wide CNDSP activities in accordance with DoDD O-8530.1, Computer Network Defense (CND).

2.5.1.1.7.2. Supports USCYBERCOM in Mission Analysis development.

2.5.1.1.7.3. Provides functional expertise in Mission Analysis, leveraging established doctrine, tactics, techniques and procedures.

2.5.1.1.7.4. Develops and implements procedures to coordinate with NOSs, MCCCs/ACCCs (if applicable), CFPs and other AF organizations to collect

timely and accurate information and to ensure effective C2 of executed COAs.

2.5.1.1.7.5. Notifies MCCCs and NOSs of cyber incidents occurring in their respective AORs to facilitate mission impact analysis. NOSs will coordinate through the 624 OC with 24 AF, if necessary, to determine if additional protections are required to prevent future similar incidents.

2.5.1.1.8. 24 AF operates the appropriate key weapon systems and associated infrastructure to support cyber incident handling. Air Force Cyber Defense (ACD) performs continuous operations to prevent, detect and respond to intrusions and attacks against Air Force networks.

2.5.2. **Air Combat Command (ACC).** AF intelligence, surveillance, and reconnaissance (ISR) assets belonging to 25th AF (ACC) provide foreign cyber threat Indications and Warnings (I&W), Attack Sensing & Warning (AS&W), in-depth entity profiling, in-depth incident analysis, and detailed sensor data analysis of foreign threats to AF computers for the ACD weapon system and 624 OC. This information is reported in a Network Intelligence Report (NIR), threat tipper, or AS&W advisory.

2.5.3. **I-NOSCs.** The I-NOSC is one of three functions provided by the Cyberspace Security and Control System (CSCS). There are three I-NOSCs: they are operated by the 83d Network Operations Squadron (83 NOS), the 561st Network Operations Squadron (561 NOS), and the Air National Guard's 299th Network Operations Security Squadron (299 NOSS). In support of DCO operations, I-NOSCs provide commanders real-time situational awareness of the network within their area of responsibility. The I-NOSCs:

2.5.3.1. Coordinate with and inform MCCCs/ACCCs (if applicable) and CFPs under their purview in response to DCO events that cross their area of responsibility. Accomplish tasking using the most expeditious means available (voice, electrical message, ACT, etc.), and direct organizations to report completion of required actions.

2.5.3.2. Report suspected/confirmed events to the ACD units in accordance with standing rules of engagement.

2.5.3.3. Coordinate with and inform the 624 OC, MCCC, CFP, and appropriate weapon system units on all corrective actions associated with the investigation and mitigation of events and incidents.

2.5.4. **MCCCs.** MCCCs, or similar structures established at the discretion of the MAJCOM, provide network situational awareness to MAJCOM/CCs and manage MAJCOM-unique systems and applications. MCCCs:

2.5.4.1. Coordinate with the functional communities within their area of responsibility to maintain a situational awareness picture of all MAJCOM-unique systems and applications on AF networks.

2.5.4.2. Coordinate DCO and DoDIN Operations COA planning and execution with the appropriate I-NOSC, the 624 OC and applicable 24 AF-designated units as appropriate. Provide operational impact data to assist efforts to investigate and mitigate events and incidents involving systems within their area of responsibility.

2.5.5. **CFPs/Communications Squadrons.** CFPs, and those Communication Squadrons at locations without a servicing CFP, provide an on-site technical capability to implement

physical and logical network changes, modifications, and restoration of faulty network transmission equipment and circuits. CFPs implement Cyber Tasking Orders (CTOs) and messages received from the 624 OC and/or the AFSPC Command Center. CFPs:

2.5.5.1. Execute the operational direction of the 624 OC and CSCS units for DCO and DoDIN Operations COA development and execution. Coordinate with and inform the lead C3MS unit, MCCC/ACCC (if applicable), and other tasked/participating units on all corrective actions associated with the investigating and mitigation of events and incidents.

2.5.5.2. Provide the servicing ACCC/MCCC (if applicable), CSCS units, ACD units, and 624 OC all necessary information and data (i.e., system and anti-virus logs) requested to assist with incident/event investigations within the timelines specified. If unable to provide the necessary information/data or meet the specified timelines due to technical limitations or other factors, provide a detailed explanation (along with a get well date, if applicable) to the 624 OC, CSCS units, ACD units, other tasked/participating units, and ACCC/MCCC (if applicable), for tracking, COA modification, and trending purposes.

Chapter 3

INCIDENT HANDLING

3.1. General. Units operating the ACD and AFINC weapon systems monitor and record suspicious and unauthorized network and information systems access and activity on AF networks. Suspicious activity may include network scanning, multiple connection attempts to a network device from an unknown entity, or other reportable activity detected at any level. Intrusion activity may include the presence of unusual or excessive activity on the network, or unauthorized individuals gaining full (root) or limited (user) access to a network device or information system. Report data spillages and classified message incidents as a security incident in accordance with AFI 16-1404, *Air Force Information Security Program*.

3.2. Incident Handling Process and Life Cycle. The basic process for cyber incident handling consists of six phases:

3.2.1. Detection and reporting of events.

3.2.2. Preliminary analysis and identification.

3.2.3. Preliminary response actions.

3.2.4. Incident analysis.

3.2.5. Response and recovery.

3.2.6. Post-incident analysis.

3.3. Detection and Reporting of Events. The AF detects activity through a variety of means and capabilities. These range from detection via weapon systems utilizing network intrusion detection/prevention sensors to local personnel identifying questionable activity via Enterprise Information Technology Service Management (EITSM) records, trend analysis, or problem management investigations. Depending upon the identifying source and method used to detect the activity, all affected parties and tasked units gather/report preliminary information and coordinate reporting and response actions among themselves and with other organizations as appropriate.

3.3.1. **Objectives.**

3.3.2.1. Ensure all suspicious activity is detected and reported so that further analysis can take place to determine if it is a reportable event or incident.

3.3.2.2. Ensure suspicious activity is reported in a timely manner consistent with required reporting timelines. Reporting accurate incident information as close to near-real-time as possible is crucial to an effective response. If the incident meets OPREP-3 criteria, report the operational impact in accordance with AFI 10-206, Operational Reporting, **Chapter 3**.

3.3.2.3. Coordinate with command channels, DoD organizations, and assigned Authorizing Officials (AO) or their staffs as required.

3.4. Preliminary Analysis and Identification. Upon detection of a possible event by internal or external sources, the 624 OC and ACD units will initiate notification procedures in accordance with AFI 10-206, CJCSM 6510.01B, and established Standard Operating Procedures

(SOPs) of the affected units **(T-2)**. Notification messages must be properly classified (see paragraph 3.4.4.3 below) **(T-2)**.

3.4.1. Refer to paragraph 4 for guidance on identifying exercise incidents/events reported, and the processes for de-conflicting real world and exercise activities.

3.4.2. In cases when the cause/intent of a possible event is not readily apparent, initially categorize detected activity as a CAT 8 investigation. During this time, the ACD unit coordinates with the 624 OC, and other participating units, as applicable, to gather additional information to assist in the investigation. Information typically requested during the course of an investigation includes: data showing the true source of system affected by the activity, anti-virus and system log data, and initial forensics data obtained either remotely or locally by using appropriate forensics tools as directed. The ACD unit may also request the victim system's hard drive for an in-depth forensic analysis.

3.4.2.1. As the investigation of an event progresses and additional information is obtained, the assigned category may be changed to reflect the new data. For example, an initial CAT 8 event may be re-designated as a root-level intrusion (CAT 1 incident) or a result of non-compliance activity (CAT 5 event).

3.4.2.2. In order to support incident investigation, CSCS units and other applicable units will retain proxy server, firewall and Domain Name Server audit logs for a minimum of one year in accordance with the AF Records Disposition Schedule, Series 33, Table 25, Rule 8.00 (T 33-25 R 8), unless a longer retention period is specified in other guidance **(T-2)**.

3.4.2.3. Upon detecting a suspected or verified incident, notify the Primary Recipient according to the guidance in Table 3.1.

Table 3.1. Incident Reporting Action Matrix.

If the originator / recipient of the incident report (IR) is	then take the indicated Actions	and the Primary Recipient will be	and Informational Recipients will be
End user	1	Client Support Technician (CST)/ Cybersecurity Liaison (CSL)	N/A
CST/CSL	2, 7	CFP	Supporting NOS
Functional System Administrator (FSA)	2, 7	CFP	ACCC/MCCC/NOS
NCC/CFP	2, 7	Appropriate CSCS unit, ACCC/MCCC	624 OC, ACD unit
I-NOSC	3-7	624 OC	ACD unit, ACCC/MCCC

Actions	
1	Upon detection of an incident, end users will immediately notify their assigned CST/CSL and provide information as requested. **(T-2)**
2	Upon detection or notification of an incident, the CST/CSL will notify their servicing CFP. After notifying the CFP, the CST/CSL will prepare and transmit an IR to the servicing CFP. If there is no servicing CFP, send the IR directly to the supporting I-NOSC. Support the ACD unit as directed during investigation of incident. **(T-2)**
3	Upon detection or notification of an incident, contact the 624 OC for assessment of the incident and assignment of an Incident Report Identifier (IRID) (upon validation). **(T-2)**
4	After making initial contact with the 624 OC, follow-up by submitting an initial IR. **(T-2)**
5	Submit an updated IR every 7 days until all actions required to resolve the incident are complete. **(T-2)**
6	Submit a final IR within 24 hours of the all action related to the incident being completed. **(T-2)**
7	Send an informational copy of all IRs to the Informational Recipients indicated. **(T-2)**

3.4.3. **Objectives.**

3.4.3.1. Determine whether a detected event is a reportable event or incident.

3.4.3.2. Ensure all appropriate DoD organizations, to include assigned Authorizing Officials (AO) and their staffs, are notified through technical and operational reporting channels.

3.4.3.3. Ensure the timely submission, by the organization that first discovers and reports the incident, of an initial incident report that contains as much complete and useful information as is available (or possible). This includes timely submissions into the DoD's Joint Incident Management System (JIMS).

3.4.4. **Methodology.**

3.4.4.1. Assess and Categorize. Assess the event against the incident criteria to determine if it is a reportable event or incident (See Table 1.1, Incident Categories). In cases where more than one category applies, use the category of highest precedence as outlined in the Table 1.1.

3.4.4.2. Classification of Incident Reports. Incident reports may be either classified or unclassified. The individual responsible for developing the incident report will review either DoDI O-3600.02 or the AF Cyberspace Operation Security Classification Guide (SCG) to determine if the report should be classified. **(T-1)** If it is determined the report is unclassified the author should mark the report in accordance with AFI 16-1404 using the standards for controlled unclassified information. The author may contact the Wing Information Protection Office for additional guidance on marking reports.

3.4.4.3. Based on the incident category, nature, and impact of the incident, determine if the computer forensics process should be initiated per CJCSM 6510.01B **(T-2)**.

3.5. Preliminary Response Actions. Preliminary response actions are the immediate steps taken once an incident has been detected and declared. They provide information to help protect the systems and network from more damage while more detailed analysis is completed. More detailed response steps may be taken after a more thorough analysis is performed. These will be based on the nature, scope, and potential impact of the incident. Preliminary response actions should not result in a self-imposed denial of service; that is, wherever possible, affected systems/networks should be kept in operation to support the unit mission.

3.5.1. **Objectives.**

3.5.1.1. Isolate and contain the reportable event from causing further damage to AF networks.

3.5.1.2. Maintain control of the affected system(s) and surrounding environment.

3.5.1.3. As directed by AFOSI and the 624 OC, begin chain of custody documentation and ensure forensically sound acquisition of required data as determined by preliminary analysis and identification; reference paragraphs 3.4.2 and 3.5.2.5.

3.5.1.4. Maintain and update the incident report and communicate updates through the appropriate technical and operational command channels.

3.5.1.5. AFOSI will notify ACD unit preliminary responders if AFOSI will conduct an investigation. If AFOSI elects to conduct a criminal investigation or counterintelligence operation, ensure data acquisition, storage and release is conducted according to case agent (in consultation with 624 OC) direction. Resulting data may be controlled as Law Enforcement Sensitive (LES) and details will be provided to those with a need to know via trusted agents. **(T-2)**

3.5.2. **Methodology.**

3.5.2.1. Network technicians and incident handling personnel contain the incident and/or potential threat to protect the affected system or network and prevent any further contamination, intrusion, or malicious activity.

3.5.2.1.1. Containment can be done by an automated detection system or by incident handling staff working in conjunction with technical and management staff.

3.5.2.1.2. Network technicians and incident handling personnel coordinate containment with the supporting CNDSP. The commander and supporting CNDSP will coordinate with LE/CI when initial investigation indicates the possibility of criminal or hostile intelligence activity **(T-2)**.

3.5.2.1.3. Carefully decide on containment actions that may affect the ability to acquire and preserve data about the incident. When making these decisions, it is important to assess the relative value of ensuring mission success by preventing further damage against the potential for containment actions to hinder further analysis.

3.5.2.2. Acquire and Preserve Data. Safely acquire and preserve the integrity of all data (as directed by incident handling, law enforcement, or counterintelligence personnel) to allow for further incident analysis. This may include making primary and working images(s) of affected system(s) in a forensically sound manner as directed by AFOSI, the supporting CNDSP, or the 624 OC.

3.6. Incident Analysis . Incident analysis is a series of analytical steps taken to find out what happened in an incident. Include the mission owner in the process. The purpose of this analysis is to understand the technical details, root cause(s), and potential impact of the incident. This understanding helps determine what additional information to gather, coordinate information sharing with others, and facilitate working with the MAJCOM and other organizations as needed to develop a COA for response and prevention.

3.6.1. **Objectives.**

3.6.1.1. Ensure the accuracy and completeness of incident reports.

3.6.1.2. Characterize and communicate the potential impact of the incident. This includes identifying and sanitizing any compromised AF data.

3.6.1.3. Systematically capture the methods used in the attack and identify security controls that could prevent future occurrences.

3.6.1.4. Research actions that can be taken to respond to and eradicate the risk and/or threat.

3.6.1.5. Understand patterns of activity to characterize the threat and direct protective and defensive strategies.

3.6.1.6. Identify the likely root cause(s) of the incident through technical analysis.

3.6.2. **Methodology.**

3.6.2.1. Gather information. All involved personnel should identify and collect all relevant information about the incident for use in incident analysis. Information gathered may include data previously acquired and preserved, external logs, personal accounts, all-source intelligence, technical information, or the current operational situation.

3.6.2.2. Validate the incident. Personnel should continuously review, corroborate, and update (if applicable) the reported incident to ensure the accuracy of all information.

3.6.2.3. Determine the operational impact. Operational impact refers to detrimental impacts on an organization's ability to perform its mission. This may include direct and/or indirect effects that diminish or incapacitate system or network capabilities, the compromise and/or loss of mission critical data, or the temporary or permanent loss of mission critical applications or systems. Coordinate as necessary with the HQ USAF Damage Assessment Management Office (AF-DAMO), the lead CDA unit for Cyber Operations Risk Assessments (CORA), or other organizations for assistance in preparing an impact assessment.

3.6.2.4. Coordinate with the victim system's owning CFP, NOS, and MCCC (as appropriate) to determine the Mission Assurance Category level of the system.

3.6.2.5. Determine within one hour if the event or incident meets AF Operational Reporting (OPREP-3) and/or USSTRATCOM or USCYBERCOM Commander's Critical Information Requirements (CCIR) reporting requirements.

3.7. Response and Recovery. Response and recovery includes the detailed response steps performed to prevent further damage, restore the integrity of affected systems, and implement follow-up strategies to prevent the incident from happening again. The local CFP, with the assistance of the mission owner, the servicing MCCC/ACCC and applicable CSCS units, will develop a Plan of Action and Milestones (POA&M) detailing the required actions and responsible offices/individuals to guide system restoration and prevention of similar incidents in the future **(T-2)**.

3.7.1. **Objectives.**

3.7.1.1. Resolve the incident according to this instruction, CJCSM 6510.01B, and local guidance.

3.7.1.2. Eliminate the risk or threat.

3.7.1.3. Either restore the integrity of the system and return it to an operational state, or properly destroy the information/media according to AFMAN 17-1301, *Computer Security (COMPUSEC)*.

3.7.1.4. Implement proactive and reactive defensive and protective measures to prevent similar incidents from occurring in the future. Coordinate with the appropriate AFSPC Weapon System Team Leads to ensure that lessons learned can be used to improve existing capabilities or justify the development of new ones.

3.7.1.5. Collaborate with LE or IC partners to identify investigative or intelligence equities which may need to be considered before certain containment measures are taken.

3.7.2. **Methodology.**

3.7.2.1. If applicable, implement additional containment actions to regain control of or isolate the system and prevent further malicious activity.

3.7.2.2. Containment strategies vary based on the type of incident. Common strategies include restoring the compromised system to a pristine condition and/or formally decommissioning the system if it cannot be restored.

3.7.2.3. Examples of strategies include modifying network access controls (e.g., firewall), installing new antivirus or intrusion detection/prevention sensor signatures, or making physical changes to the infrastructure. As more network intrusion prevention sensors are added to the AF toolbox, assigned ACD, AFINC, and CSCS weapon system units will, as directed by the 624 OC, determine the appropriate thresholds for automated/real-time blocking of suspect activity **(T-2)**. The 624 OC should coordinate with MAJCOMs, Air National Guard (ANG), and numbered air force/warfighting headquarters to review and adjust blocking thresholds as needed.

3.7.2.4. The decision to restore a system without identifying the root cause(s) of an incident must be weighed carefully as it may leave the system vulnerable. Local commanders, with the assistance of the supporting communications element, will determine the adequacy of final restoration or decommissioning actions, and are responsible for ensuring the actions are completed **(T-2)**.

3.7.2.5. Applicable ACD, CSCS, and AFINC weapon system units, MCCCs/ACCCs, and CFPs conduct scans, as capabilities permit, to ensure fix actions are complete, Technical Orders (TOs) are implemented, and all known vulnerabilities are patched/mitigated.

3.7.3. **Post-Incident Analysis.**

3.7.3.1. Post-incident analysis involves the postmortem analysis of an incident to review the effectiveness and efficiency of incident handling. Data captured in the postmortem includes lessons learned, initial root cause, problems with executing COAs, missing policies and procedures, and inadequate infrastructure defenses. Post-incident analysis reporting will be provided to the affected MAJCOM/unit so that corrective actions can be taken **(T-2)**.

3.7.3.2. The ACD unit drafts a Cyber Incident Report (CIR), which provides a detailed analysis to include the affected system, probable attacker, attack vector used, and technical and operational impacts (if known). A general CIR format with detailed instructions can be found in CJCSI 6510.01B, Appendix B to Enclosure C.

3.7.3.3. 25AF provides intelligence support to the ACD unit CIR incident reporting process through the production of a Network Intelligence Report (NIR), an all-source report which focuses on an incident, group of incidents, or network activity or on a foreign individual, group, or organization identified as a threat or potential threat to DOD networks. A general NIR format with detailed instructions can be found in CJCSI 6510.01B, Appendix B to Enclosure F.

3.8. LE & CI Incidents . An incident/event investigation involving LE/CI (e.g., investigation of insider activity) may deviate from "typical" cyber incident handling processes depending upon the nature and sensitivity of the investigation. In such cases, information may be "law enforcement sensitive" or subject to other handling restrictions, with limited distribution to the general AF community.

3.8.1. An incident/event investigation involving the IC may deviate from "typical" cyber incident handling processes depending upon the nature and sensitivity of the operation. In such cases, adversary activity may be allowed to continue in order for friendly forces to gain actionable intelligence or allow for the continuation of friendly classified operations.

Table 3.2. Incident Handling and Support Activities.

This table presents the relationship between the ongoing support activities and the basic phases of incident handling.			
	Reporting & Notification	Documentation	Coordination
Detection of Events	Submission of report of events of interest	Initial documentation of event activity	Global information sharing and gathering between tiers, with other DCO and DoDIN Operations components, LE/CI or IC
Preliminary Analysis & Identification	Submission of initial incident report	If no documentation has been started initial documentation should occur here	Coordination to identify additional sources of information and artifacts
Preliminary Response Action	Update of actions taken	Documentation of any actions taken	Coordination of technical and organizational steps taken to implement preliminary actions across all affected C/S/As
Incident Analysis	More detailed updates of analysis performed	Documentation of analysis results	Coordination of incident analysis activities between DCO, DoDIN Operations, mission owners, technical and management components and internal/external subject matter experts
Response & Recovery	Updates on actions taken and submission of final report for closure	Documentation of response plan, analysis performed, and COAs	Coordination of response actions between C/S/As and field activities, CNDSPs, mission owners, Installations and DCO Service subscribers, DoDIN Operations, and with LE/CI and IC, and others as required
Post-Incident Analysis	Submission of Post-Incident Analysis report	Documentation of lessons learned and resulting improvement plan	Coordination between DoD components to implement any process improvement activities resulting from post-incident analysis

Chapter 4

EXERCISES

4.1. Exercises on Operational Networks. Organizations that conduct exercises on operational networks run the risk of confusing exercise incidents with real world incidents. Any organization that participates in exercises conducted on operational networks will ensure procedures are in place to manage real world and exercise incidents.

4.2. Joint Exercises. The sponsoring command should provide the rules of engagement (ROEs) and standard operating procedures (SOPs) for the exercise. The senior Air Force representative from each participating organization will ensure the ROEs and SOPs address the issue of managing real world and exercise events and incidents. Participating organizations will attend planning conferences to ensure their equities are represented.

4.3. Air Force Exercises. The sponsoring command will establish the ROEs and SOPs for the exercise participants and will ensure the ROEs and SOPs address the issue of managing real world and exercise events and incidents. Participating organizations will attend planning conferences to ensure their equities are represented.

4.4. MAJCOM Exercises. The sponsoring MAJCOM Staff element will establish the ROEs and SOPs for the exercise participants and will ensure the ROEs and SOPs address the issue of managing real world and exercise events and incidents. Participating organizations will attend planning conferences to ensure their equities are represented.

4.5. Internal Exercises. Organizations conducting internal exercises on operational networks will establish the ROEs and SOPs for the exercise participants.

MARK. C. NOWLAND, Lt Gen, USAF
Deputy Chief of Staff, Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 3600.01, *Information Operations*, 2 May 2013

DoDD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, 21 October 2010

DoDD 5400.11, *DoD Privacy Program*, 29 October 2014

DoDD 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3),* 1 March 2010

DoDD O-8530.1, *Computer Network Defense (CND),* 8 January 2001

DoDD O-8530.1-M, *DoD Computer Network Defense (CND) Service Provider Certification and Accreditation Process,* 8 January 2001

DoDI O-3600.02, *Information Operations (IO) Security Classification Guidance*, 28 November 2005

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDI O-8530.2, *Support to Computer Network Defense (CND),* 9 March 2001

Office of the Secretary of Defense (OSD) Memorandum OSD 06227-09, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, 5 June 2009

CJCSI 3121.01B, *Standing Rules Of Engagement/Standing Rules For The Use Of Force For US Forces*, 13 Jun 2005

CJCSI 3213.01D, *Joint Operations Security*, 7 May 2012

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* 09 February 2011

CJCSM 6510.01B, *Cyber Incident Handling Program,* 10 July 2012 (current as of 18 December 2014)

National Security Telecommunications and Information Systems Security Directive 503, *Incident Response and Vulnerability Reporting for National Security Systems Security*

Committee on National Security Systems (CNSS) Instruction 4009, Jun 06 (revised 26 April 2010)

JP 3-12, *Cyberspace Operations*, 5 February 2013

AF Doctrine Annex 3-12, *Cyberspace Operations,* 30 November 2011

AFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, 8 March 2007

AFPD 17-2, *Cyberspace Operations,* 31 July 2012

AFI 10-206, *Operational Reporting*, 11 June 2014

AFI 17-201, *Command and Control for Cyberspace Operations*, 5 March 2014

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 17-100, *Air Force Information Technology (IT) Service Management*, 16 September 2014

AFI 17-130, *Air Force Cybersecurity Program Management*, 31 August 2015

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 27 March 2012

AFI 33-332, *The Air Force Privacy and Civil Liberties Program*, 12 January 2015

AFMAN 33-363, *Management of Records*, 1 March 2008

USAF Interim Computer Network Attack (CNA) Security Classification Guidance, 3 June 2002, with Change 2, 1 June 2006

Adopted Form

AF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

25AF—25th Air Force

624 OC—624 Operations Center

ACC— Air Combat Command

ACCC— AFFOR Communications Coordination Center

ACT—AFNETOPS Compliance Tracker

AETC— Air Education and Training Command

AF— Air Force

AFCERT— Air Force Computer Emergency Response Team

AFCYBER—Air Forces Cyber (24AF)

AFDD— Air Force Doctrine Document

AFI— Air Force Instruction

AFIN— Air Force Information Network

AFMAN—Air Force Manual

AFMC— Air Force Materiel Command

AFNIC— Air Force Network Integration Center

AFOSI— Air Force Office of Special Investigations

AFPD— Air Force Policy Directive

AFRC— Air Force Reserve Command

AFSPC— Air Force Space Command

ANG— Air National Guard

C2— Command and Control

CAT— Category (i.e., CAT 1 root level intrusion)

CCDR— Combatant Commander

CCIR— Commander's Critical Information Requirements

CERT— Computer Emergency Response Team

CFP—Communications Focal Point

CI— Counterintelligence

CIO— Chief Information Officer

CIR— Cyber Incident Report

CJCS— Chairman, Joint Chiefs of Staff

CJCSI— Chairman, Joint Chiefs of Staff Instruction

CJCSM— Chairman, Joint Chiefs of Staff Manual

CNDSP— Computer Network Defense Service Provider

CNA—Computer Network Attack

CNSS—Committee on National Security Systems

COA— Course of Action

CoR— Certificate of Reconstitution

CORA— Cyber Operations Risk Assessment

C/S/As— Combatant Commands/Services/Agencies

CSL—Cybersecurity Liaison

CST—Client Service Technician

CTO— Communications Tasking Order

DC3—Defense Cyber Crime Center

DCO— Defensive Cyberspace Operations

DoD— Department of Defense

DoDD— Department of Defense Directive

DoDI— Department of Defense Instruction

DoDIN—Department of Defense Information Networks

EITSM— Enterprise Information Technology Service Management

HQ— Headquarters

I&W— Indications & Warnings

IA— Information Assurance

IC— Intelligence Community

I—NOSC – Integrated Network Operations Security Center

IO— Information Operations

IP—Information Protection

IS—Information System

ISR— Intelligence, Surveillance, and Reconnaissance

IT—Information Technology

JIMS—Joint Incident Management System

JP— Joint Publication

LE— Law Enforcement

MAJCOM— Major Command

MCCC— MAJCOM Communications Coordination Center

NOS—Network Operations Squadron

OPR— Office of Primary Responsibility

PII—Personally Identifiable Information

SOPs— Standard Operating Procedures

TCTO— Time Compliant Technical Order

TO— Technical Order

USAF— United States Air Force

USCYBERCOM—United States Cyber Command

USSTRATCOM—United States Strategic Command

Terms

Attack Sensing and Warning (AS&W)—The detection, correlation, identification and characterization of intentional unauthorized activity, including computer intrusion or attack, across a large spectrum coupled with the notification to command and decision makers so that an appropriate response can be developed. Attack sensing and warning also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments.

Classified Message Incident.—A form of data spillage which results when classified information is transmitted over unclassified channels, or via channels not approved for its level of classification.

Client Support Technician (CST).—An individual who supports customers with resolving issues relating to information technology devices, such as personal computers, personal digital assistants, and printers. (AFMAN 17-1201)

Counterintelligence (CI).—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. (DoDI 5200.1-R)

Cyber (adj.).—Of or pertaining to the cyberspace environment, capabilities, plans, or operations. (AFPD 17-2)

Cybersecurity Liaison.—An individual responsible for ensuring that the appropriate operational cybersecurity posture is maintained for an AF information system or organization. (AFI 17-130)

Cyberspace.—A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02)

Cyberspace Operations—The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-12)

Data Spillage—Spillage occurs when classified data is entered into a system/device not accredited for its level of classification. For example, if a user copies a classified data file to removable media (e.g. thumb drive, DVD or CD) from SIPRNET and then uploads the data onto a NIPRNET computer, spillage results.

Defensive Cyberspace Operations (DCO).—Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities. (JP 3-12)

Department of Defense Information Networks (DoDIN).—The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 3-12)

Department of Defense Information Network (DoDIN) Operations.—Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information Networks. (JP 3-12)

Event.—Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. (CNSSI 4009)

Incident.—An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (CNSSI 4009)

Indications & Warning (I&W)—Intelligence activities to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency;

nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to U.S. reconnaissance activities; terrorists' attacks; and other similar events.

Information Assurance (IA).—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 1-02)

Information Operations (IO).—The integrated employment, during military operations, of information-related capabilities (IRC's) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 13-3)

Attachment 2

AF CYBERSPACE WEAPON SYSTEMS

A2.1. There are six CSAF -approved cyberspace weapon systems with their associated infrastructure and other major systems which are impacted by this AFI. This list does not include every weapon system nor is it intended to be an all-inclusive list as new weapon systems may be introduced in the future to operate, defend and C2 the DoDIN and its operations.

A2.1.1. Air Force Cyberspace Defense (ACD). ACD prevents, detects, responds to, and provides forensics of intrusions into unclassified and classified AF networks.

A2.1.2. Air Force Intranet Control (AFINC). AFINC is the top level boundary and entry point into the Air Force Information Network (AFIN), and controls the flow of all external and inter-base traffic through standard, centrally managed gateways.

A2.1.3. Cyber Command and Control Mission System (C3MS). C3MS is the single AF weapon system providing overarching 24/7/365 awareness, management and control of the AF portion of the cyberspace domain. It ensures unfettered access, mission assurance, and joint warfighter use of networks and information processing systems to accomplish worldwide operations.

A2.1.4. Cyberspace Defense Analysis (CDA). CDA monitors, collects, analyzes, and reports on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and USAF websites. Also, CDA conducts Cyberspace Operational Risk Assessment (CORA) activities which assesses data compromised through intrusions into AF networks with the objective of determining the associated impact to operations resulting from that data loss.

A2.1.5. Air Force Cyber Security and Control System (CSCS). CSCS provides 24/7 network operations and management functions and enables key enterprise services within Air Force unclassified and classified networks.

A2.1.6. Cyberspace Vulnerability Assessment/Hunter (CVA/Hunter). CVA/Hunter executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The weapon system can perform defensive sorties world-wide via remote or on-site access.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu