Notifications

Proficiency Code: A

It's important to report insecurities and vulnerabilities immediately to prevent intrusions, damage or further damage to information systems.

Incident and vulnerability reporting procedures:

Air Force members must report information system/application vulnerabilities, security incidents, and virus attacks according to AFI 33–115, *Air Force Information Technology Service Management.* The table below shows the COMPUSEC incident and identifies reporting procedures based upon the originator of the report. As a user, you are responsible for reporting all incidents and vulnerabilities that you encounter. To start the reporting process, contact your workgroup manager for the initial report. Other areas receive notification as required.

COMPUSEC Incident and Vulnerability Reporting Procedures			
Originator	**Action**	**Primary Recipient**	**Other Security Recipients**
End-User	1	WM	CSSO, ISSO, FSA, AND NCC
CSSO/ISSO	2 – 3	NCC	Wing IA Office, NOSC, and DAA
WM	2 – 3	NCC	CSSO, ISSO, Wing IA Office, NOSC, and DAA
FSA	2 – 3	NCC	CSSO, ISSO, Wing IA Office, NOSC, and DAA
NCC	1 – 8	NOSC	Wing IA Office, DAA, and AFNOC
NOSC	1 – 8	AFCERT	MAJCOM IA Office, DAA, and AFNOC
AFNOC	1 – 8	AFCERT	N/A
PMO or SPO	2 – 3	NOSC or AFCERT	N/A

Action

1. Upon detection of an incident or vulnerability, immediately provide information to assist in filling out an initial report.
2. Notify Other Recipients as required.
3. The Computer Systems Security Officer (CSSO), Information System Security Officer (ISSO), Workgroup Manager (WM), and Functional Solution Analysis (FSA) prepares and send an initial report to the Air Force Computer Emergency Response Team (AFCERT) within 24 hours of detection.
4. Network Control Center (NCC) prepares and sends reports to their parent Network Operation Security Center (NOSC).
5. Network Operation Security Center (NOSC) and Air Force Network Operation Center (AFNOC) prepare and send initial report to the AFCERT within 24 hours of detection.
6. Prepare and send supplemental reports to the Primary Recipient as required, but at least every 30 days.
7. Prepare and send final report to the Primary Recipient within 5 days of resolution.
8. Send an informational copy of any report to the Other Recipients indicated above.

CSSO – Computer Systems Security Officer	AFNOC – Air Force Network Operations Center
ISSO – Information Systems Security Officer	PMO – Program Management Offices
WM – Workgroup Manager	SPO – System Program Offices
FSA – Functional System Administrator	AFCERT – Air Force Computer Emergency Response Team
NCC – Network Control Center	IA – Information Assurance
NOSC – Network Operations Security Center	

User’s actions after reporting:

1. User disconnects affected IS or media from the network (i.e. removal of network cable, turn off wireless capability, etc.). Do not turn off the IS. Protect the IS or media accordingly to its highest classification level of data involved.

2. User notifies organizational or system information assurance officer (IAO) or other designated representative as outlined in local operating instructions such as the unit security manager (USM), supervisor, security manager, servicing network control center, and so forth. The USM notifies the wing Information Protection (IP) office as soon as possible (preferably within 24 hours).

3. IAO or other designated representative initiates containment, which may include notification of all affected parties.

4. IAO or other designated representative begins reporting process such as the Wing IA office, unit leadership, affected server operations, and all users affected to include owners of any affected mail accounts or network user accounts.

5. IAO or other designated representative identifies key information for sanitization.

6. IAO or other designated representative hands over sanitization process to Client Support Technicians (CST) who then follows local procedures to eliminate the affected file(s).

7. IAO or other designated representatives at every level must understand this flow. IAO must educate users to this process. Basic incident response procedures are located in MPTO 00–33B–5007, *Security Incident Management for Information Systems*, Chapter 3.