IA/Cybersecurity Leader's Handbook Discussion Forum:
https://www.milsuite.mil/book/docs/DOC-73030

U.S.ARMY

AMERICA'S ARMY:
THE STRENGTH OF THE NATION™

Army Chief Information Officer/G-6
107 Army, Pentagon
Washington, DC 20310
CIOG6.Army.mil

v13.5.9b

LEADER'S INFORMATION ASSURANCE/ CYBERSECURITY HANDBOOK

ARMY CIO/G-6

IA/CYBERSECURITY IS CRITICAL TO OPERATE IN CYBERSPACE

Commanders, leaders, and managers are responsible for ensuring that Information Assurance/Cybersecurity is part of all Army operations, missions and functions. You must make certain that your organization adopts and institutes the practices necessary to ensure the protection of information and personnel.

This Handbook is designed to provide leaders the information and tools to address today's complex security challenges. It is also a quick reference for managing Cybersecurity issues that will help ensure that Soldiers, Civilians and contractors know their responsibilities for daily practices that will protect information and our IT capabilities.

WE MUST PROTECT THE NETWORK!

Information Assurance (IA)/Cybersecurity is the Army unified approach to protect the confidentiality, integrity and availability of our information and operations. IA/Cybersecurity is critical to your mission success and therefore must be part of your risk management processes. It is essential in assisting you with identifying vulnerabilities and taking the necessary steps to conduct your daily operations. Army regulations, policies and guidance provide the Army imperatives authority, responsibility and accountability necessary to promote a culture that is risk aware and complies with practices that minimize vulnerabilities to Army networks, systems and information. As leaders, you must ensure that your organization remains committed to practices that protect Army networks, systems and information as well as personnel identity.

REFERENCES AND CONTACTS

Army IA One Stop Shop:
https://InformationAssurance.us.army.mil/

IA/Cybersecurity Leader's Handbook Discussion Forum:
https://www.milsuite.mil/book/docs/DOC-73030

Army Training and Certification Tracking System (ATCTS):
https://atc.us.army.mil/

Questions regarding the ATCTS or the Army IA virtual training site can be directed to:
ciog-6netcomiawip.inbox@mail.mil

Army IA Virtual Training:
https://iatraining.us.army.mil/

Army IA Self Assessment Tool:
https://iatraining.us.army.mil/

DoD Cyber Awareness Challenge
https://ia.signal.army.mil/DoDIAA/default.asp

US Army Computer Emergency Response Team (ARCERT)
https://www.acert.1stiocmd.army.mil/

Army Home Use program
https://www.acert.1stiocmd.army.mil/Antivirus/

Army Publishing Directorate
http://www.apd.army.mil/

Army e-Learning (Skillport)
https://usarmy.skillport.com/

QUESTIONS AND TOPICS FOR YOUR IA/CYBERSECURITY TEAM

1. Ask personnel if they know who to contact with IA questions or concerns.

2. Do your people understand the importance of protecting their CAC card?

3. Question personnel about the last time they completed their DoD Cyber Awareness training. Do they require any additional certifications? If so, what's the status of those additional certifications?

4. Do your people understand Phishing, and the risk it poses to their personal and professional life?

5. Are your people using a firewall and anti-virus software on their home computers. Are they aware of the free security software that is available for their home computers? https://www.acert.1stiocmd.army.mil/Antivirus/

6. Do you include IA/Cybersecurity topics in your all-hands or town hall meetings?

7. What processes are in place to ensure personally identifiable information and sensitive/classified information is not posted on your public facing pages?

8. Conduct periodic brown bag sessions on topics such as safe home computing practices, incident reporting procedures, and using unapproved personnel devices such as smart phones and tablets to conduct official business, etc.

9. Leverage articles and cartoons from "OnCyberPatrol" website as part of your overall awareness strategy. Content can be accessed at: http://ciog6.army.mil/OnCyberPatrol.aspx

10. Lead by example and counsel people who break the rules.

INSTITUTING THE IA/CYBERSECURITY IMPERATIVES

- **Incorporate IA/Cybersecurity into your Risk Management Process**
- **Treat IA/Cybersecurity like Safety**
- **Link IA/Cybersecurity to Readiness**

As a leader, it is your responsibility to ensure that your business and information systems are protected.

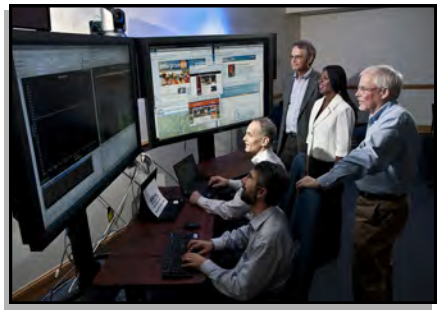
You must make certain your personnel are responsible for daily practices that protect information and IT capabilities for mission success.

It is your responsibility to assess your mission capability and practice good Cyber Hygiene - personal practices that comply with policies, process, and standards that safeguard computer use.

Remember: It is your responsibility to ensure the protection of our networks, information, and people, through increased IA training, improved Cybersecurity practices, and appropriate risk management.

EMPOWER YOUR IA/CYBERSECURITY TEAM

Know Your IA Team!



Your IA team manages your IA/Cybersecurity program.

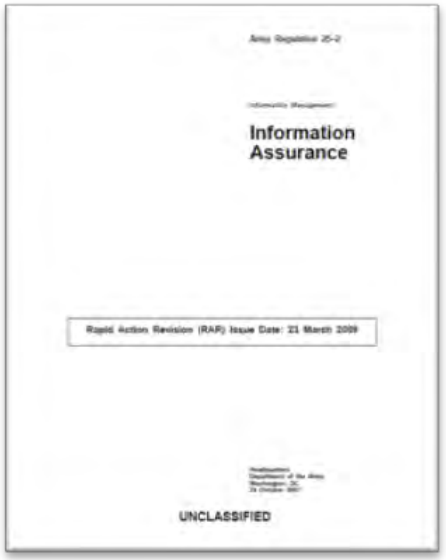
Get to know these professionals as they are key in helping you set your priorities for protecting the network and safeguarding information. Your organization must know that you make Cybersecurity a priority and understand that Cybersecurity is everyone's business.

Your IA/Cybersecurity team may include:

- **G-6/S-6 - The principle staff officer with the responsibility for the management of the commander's IA program**
- **IA Program Manager (IAPM) - Senior IA advisor to the commander**
- **IA Manager (IAM) - Implements the IA/ Cybersecurity program with assistance from the IASOs.**
- **IA Support Officer (IASO) - Provides Information Assurance oversight, guidance and support to the general user**

INFORMATION ASSURANCE ENFORCEMENT

AR 25-2 outlines sanctions that may be imposed for civilian, military and contractor personnel found in violation of Army security practices.



AR 25-2, paragraph 1-5.j states that military and civilian personnel may be subjected to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring the implementation of DoD and Army policies and procedures.

AR 25-2 further stipulates that military personnel may face administrative as well as non-judicial or judicial punishments authorized by the Uniform Code of Military Justice. Similarly, sanctions for civilian personnel may include administrative actions as well as judicial punishment. And defense contractors employees must perform under the terms of the contract and applicable directives, laws, and regulations.

INCIDENT RESPONSE

Every organization should have processes in place and the people to contact in case of an incident whether it is a security breach, information spillage, or disclosure of Personally Identifiable Information (PII). Guidelines on reporting processes are defined in AR 25-2.
http://www.apd.army.mil/pdffiles/r25_2.pdf

Common Examples of Reportable Incidents Include:

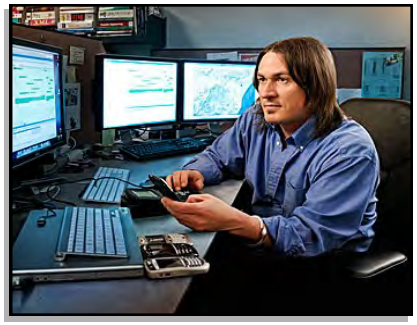
- Unauthorized Disclosure of Classified Information (spillage) - Higher-level classified information is placed on a lower level classified information system (i.e. Sending an email that contains Secret content on the NIPRNET).

US CERT has a one-hour reporting requirement for PII related incidents. Ensure your IA team's response plan meets this requirement.

- Loss or Compromise of Personally Identifiable Information (PII) - PII information that can uniquely identify, contact, or locate a single person (i.e. Posting a personnel roster which includes names, SSNs, addresses and medical information on a public website). Specific instructions on PII incidents and the reporting processes are on the Records Management and Declassification Agency's website located at: https://www.rmda.belvoir.army.mil
- Receipt of suspicious emails and phishing scams. Examples include requests to provide passwords or other sensitive information to an unknown source.

Always contact your IA team or NEC if there is any question concerning a security matter.

TRAIN YOUR PERSONNEL



Everyone must complete the appropriate training required for their position.

The Army Training and Certification Tracking System (ATCTS) provides reports and manage personnel IA training records for your IA/ Cybersecurity training management.

IA training is provided through the Army IA virtual training, and successful completion of training courses is automatically reported to the ATCTS site.

The Army IA Virtual Training site also offers training for

- Portable Electronic Devices
- Personally Identifiable Information (PII)
- Safe Home Computing

Army Training and Certification Tracking System (ATCTS): https://atc.us.army.mil/

Army IA Virtual Training: https://iatraining.us.army.mil/

DoD Cyber Awareness Challenge https://ia.signal.army.mil/DoDIAA/default.asp

Your local IA/Cybersecurity team can answer your questions about IA training requirements. Questions concerning ATCTS or the Army IA virtual training site can be directed to ciog-6netcomiawip.inbox@mail.mil.

IA/CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

Cyber Hygiene is adherence to laws and regulations, DoD and Army policies, procedures, and standards. Enforcing IA compliance is critical to strengthening the Army Cybersecurity posture.

Beyond required security training, leaders must ensure that Soldiers, Civilians and contractors understand the threat they pose to operational security with non-compliance to IA/ Cybersecurity policies and practices. People are the Army's first line of defense in sustaining good cyber hygiene and reduction in the insider threats. Most vulnerabilities and malicious acts against Army systems and information can be addressed through comprehensive and effective cyber hygiene.

Everyone is responsible for Cybersecurity!

As leaders, you must remain vigilant and constantly assess your IA/Cybersecurity posture and program with regard to readiness, risk, resources, and reporting. Have your IA/Cybersecurity team use the IA Self Assessment Tool located at https://iatraining.us.army.mil to evaluate your security posture, and report back to you with the results, and their plans to address any weaknesses identified.

RISK MANAGEMENT

Leaders must always assess potential threats and the impact on operations. Contingency plans are critical for sustaining operations through attacks or interruptions to network service.

Organizations must develop Continuity of Operations Plan (COOP) in order to maintain and sustain operations.

For your COOP to be effective, it must include:

- A Business Recovery Plan
- An Information Technology Contingency Plan
- A Facility Disaster Recovery Plan

Ensure that your plan works in conjunction with any existing COOPs adjacent to your area of control.

In addition to a fully developed COOP you must review the plans annually and practice its execution as required for the sensitivity level of the information being handled.

More information on COOPs is found in DA PAM 25-1-1.

THE COMMON ACCESS CARD (CAC)

Your CAC is your physical and digital identification; treat it as a sensitive item!

- Your CAC allows you to digitally sign emails so recipients can verify that you are the sender and the information was not altered in transit.
- Your CAC protects sensitive information in emails and computer files by allowing you to encrypt them.
- Your CAC is a physical piece of IA/Cybersecurity and is tightly bound to your online identify. Therefore, it must be protected at all times, even when not in use.
- Report a lost CAC card as soon as it's confirmed to be missing.

SIPR Tokens for SIPRNet access, have many CAC-like security capabilities and will be required to access SIPR systems. Treat it as a sensitive item and protect them as you would your CAC.

PHISHING: UNDERSTANDING THE THREAT

Everyone has seen them; an email that claims to be from a trusted source and requests your personal information, or directs you to a seemingly innocent website. These phishing attempts are usually obvious. However, phishing is a major issue that plagues the DoD and Army. Phishing is often successful because the improved quality of these attacks make it more difficult to identify them as a hoax. Phishing attacks have also become more sophisticated, targeting specific individuals with content customized specifically to them.

Everyone must be constantly aware of the phishing threat. Always be sure an email is legitimate before clicking any links or attachments, and never click any links or attachments that were received in an email that was not digitally signed.

Ensure your personnel annually complete the anti-phishing course located at:
https://iatraining.us.army.mil/

SECURING THE SYSTEM

The Internet poses serious potential threats. We must constantly ensure all computers and devices meet the appropriate security requirements before connecting them to the network.

All office and home computers must be up to date with required system security patches, Anti-Virus software application, and should only be connected to the internet from behind a firewall.

The Army Home Use program makes it easy for Army Soldiers and Government Civilians, to secure their home computers by giving them free access to both Symantec and McAfee anti-virus and firewalls.

https://www.acert.1stiocmd.army.mil/Antivirus/

Protecting your home computer with current antivirus applications and connecting to the internet from behind a firewall, are vital to preventing malware from infecting your computer.

You should discuss with personnel the importance of IA/ Cybersecurity on their home computers. Ensure they are aware of the free resources available to soldiers and government civilians, and are practicing good Cyber Hygiene both at work and at home.

PERSONAL MOBILE DEVICES

Department of Defense and Army policies prohibit connecting unauthorized information systems to the network, and prohibit conducting official business on personally owned devices that do not meet Army standards and certification requirements.

Although the Army is currently considering a strategy to allow personal mobile devices access to the Army Network, personal cell phones, tablets or other mobile devices are currently not authorized for access and government use. Using unapproved devices for official business is not only a security violation, but could also cause major security incidents jeopardizing sensitive information and putting our operations and personnel at risk. Compromising classified information in these cases is a serious security violation that may result in punitive actions.

More information on personal mobile devices can be found at:
https://informationassurance.us.army.mil/