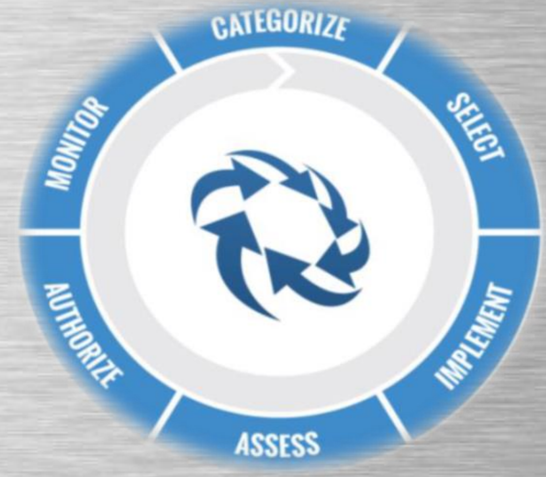
*Army Enterprise Resource Planning (ERP) integration efforts*

*Logistics Modernization Program (LMP)*

# Cybersecurity

## (Information Assurance)

**Standard Army Maintenance System-Enhanced**



Eric Hoover
United States Army Materiel Command
Eric.d.hoover2.civ@mail.mil
309.782.1077

# Agenda

- Cybersecurity
- Defense Science Board
- Threat Scenario
- Cybersecurity - Information Assurance
- Cybersecurity – A Team Sport and Responsibility
- What is a Breach?
- Types of Breaches/Incidents
- Threats Against Information Systems
- Operational Resilience, Integration, and Interoperability
- Mobile Environment = On the Road
- Top Ten Rules

# Cybersecurity

Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Department of Defense Instruction (DoDI) 8500.01, March 14, 2014

DoDI 8500.01 adopts the term “cybersecurity” to be used throughout the DoD instead of the term “information assurance (IA).”

# Defense Science Board
# Cybersecurity Observations

“Current DoD actions though numerous are fragmented. Thus, DoD is not prepared to defend against this threat.”

“DoD Red Teams, using cyber attack tools which can be downloaded from the internet, are very successful at defeating our systems.”

“With present capabilities and technology, it is not possible to defend with confidence against the most sophisticated cyber attacks.”

“It will take years for the Department to build an effective response to the cyber threat.”

# Threat Scenario

Nearly every U.S. arms program found vulnerable to cyber attacks

BY ANDREA SHALAL

WASHINGTON Tue Jan 20, 2015 8:04pm EST

“The continued development of advanced cyber intrusion techniques makes it likely that determined cyber adversaries can acquire a foothold in most (Department of Defense) networks, and could be in a position to degrade important DOD missions when and if they chose to.” Michael Gilmore, Director of Operational Test and Evaluation (DOT&E).

# Threat Scenario

Mobile

Cross Platform

Wireless

Social Media

# Cybersecurity - Information Assurance

Protect Army information and Readiness from theft

Protect the network from hackers and viruses

Protect systems through inspection and certification

- Leadership and Cybersecurity Professionals
- Software Assurance
- Supply Chain Risk Management
- Cybersecurity, a Team Sport

***Confidentiality – Integrity - Availability***

# Cybersecurity – A Team Sport and Responsibility

## Who should be involved and how?

Test and Evaluation    Maintenance    Manufacturing

Cybersecurity Professional    Engineers

Machine Operators    Contracts    Program Manager

Leadership    Quality    Logistics

**Cybersecurity in the DoD workforce requires vigilance from everyone who communicates information digitally. It is a true team sport that affects everyone's job, and it is the responsibility of the entire DoD workforce.**

# What is a Breach?

Suspected loss, loss, or compromise of information will be referred to as a breach. A breach incident occurs when it is suspected or confirmed that information is lost, stolen, or otherwise made available to individuals without a duty-related official need to know.

# Types of Breaches/Incidents

- Types of breaches/incidents include, but are <u>not</u> limited to:
  - Losing federal, contractor, or personal electronic devices that store information (e.g., laptops, cell phones that can store data, disks, Blackberry, compact disks, etc.)
  - Sharing paper or electronic documents containing information with unauthorized individuals
  - Posting to a public website (intentionally or unintentionally)
  - Mailing hard copy documents containing to the incorrect address
  - Leaving documents containing controlled information exposed in an area where individuals without approved access could read, copy or move for future use

# Threats Against Information Systems

- Unauthorized Activities
  - Download of programs/files
  - Use of Instant Messaging, peer to peer (file sharing) or chat services
  - Note: We have been testing Microsoft Office Communicator for internal chatting

- Virus Attacks (email or web)
  - Don’t open email from suspicious sources
  - Avoid surfing the Web

- Peripheral Storage Devices
  - Flash Drives, Thumb Drives, and MCP players must be blocked

# Operational Resilience, Integration, and Interoperability

## Operational Resilience

- Information and computing services are available to authorized users whenever and wherever needed
- Security posture is sensed, correlated, and made visible to mission owners, network operators, and to the DoD Information Enterprise
- Hardware and software have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention

## Integration and Interoperability

- Cybersecurity must be fully integrated into system life cycles and will be a visible element of IT portfolios.
- Interoperability will be achieved through adherence to DoD architecture principles
- All interconnections of DoD IT will be managed to minimize shared risk

# Mobile Environment = On the Road

- Carry a Property Pass, Optional Form 7, signed by your hand receipt holder, when taking laptop off post
- Carry a copy of the RIA Authority to Operate (ATO) in case questioned at another site
- Make sure you always use VPN for remote access
- Make sure you keep your laptop with you or locked up at all times
- Make sure your laptop is marked with both a Data at Rest (DAR) and Unclassified sticker
- If going to another DoD installation with plans to connect your laptop, check with the IA Teams 1-2 weeks before about getting your notebook scanned and obtaining a copy of a compliance memorandum.

# Top Ten Rules

1. Do not email Classified information or post on websites or access classified information unless on a SIPR computer.

2. Download only work related information.

3. Be suspicious of e-mail and attachments from unknown sources - Verify digital signatures.

4. Encrypt all For Official Use Only (FOUO), PII and sensitive data.

5. Never share Common Access Card (CAC) pins or passwords.

6. Lock up passwords - Do not display anywhere on your computer station or notebook.

# Top Ten Rules

6. Remove your CAC when leaving your machine and keep it with you at all times.
7. Do not use Universal Serial Bus (USB) devices.
8. Do not use unauthorized Peer-to-Peer, Instant Messaging or Chat Services. Avoid Social Networking sites.
9. Immediately report any computer virus, infection or unusual computer behavior to the IA Team.
10. Take your Annual Information Assurance Training as directed.

# Questions