CIOG6.ARMY.MIL

Cybersecurity: The Defense Perspective

CIO/G-6
ENABLING SUCCESS
For Today and Tomorrow

Ms. Essye Miller

Director, Cybersecurity Army CIO/G-6

October 15, 2015

CIO/G-6

As the CIO

Reports directly to the **Secretary of the Army** for setting the strategic direction and objectives, and supervising all Army C4 and information technology functions.

As the G-6

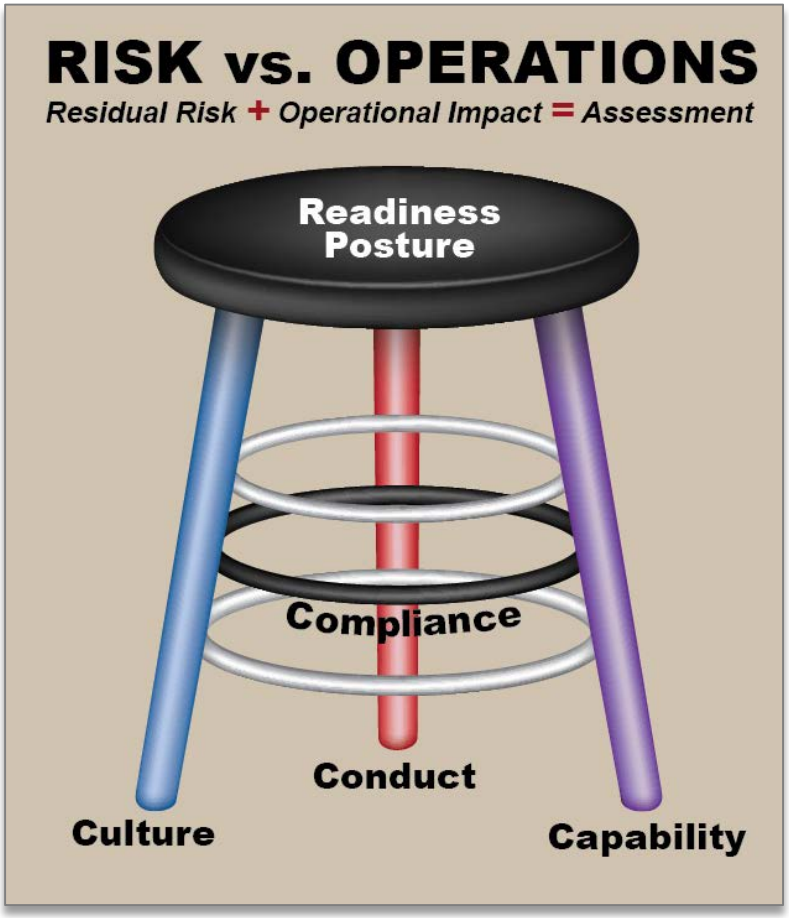
Supports the **Chief of Staff** and the Army to enable expeditionary mission command; network defense and operations; and restructure, equip and employ Signal forces.

Cyber Security

- Army Cyber Strategy
- Information Assurance
- Cyber Emerging Technologies / R&D
- Testing, Evaluation & Certification
- Integrates Cyber Security & Network Modernization

Culture, Conduct, & Capabilities

- **Culture:**
  - Statutes
  - Policy & Doctrine,
  - Directives, Regulations, & Orders
- **Conduct:**
  - Awareness
  - Training (Individual & Organizational)
  - Discipline
- **Capability:**
  - Enterprise
  - Enclave (Post/Camp/Station/ Community of Interest)
  - End Point

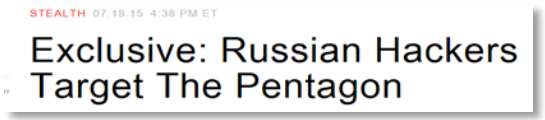


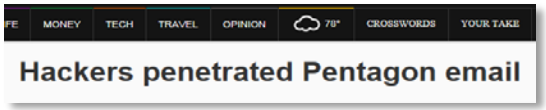
Culture

- **US Statutes:**
  - Title 40 USC - The Clinger Cohen Act of 1996
  - Title 44 USC - The Federal Information Security Management Act 2002
  - Title 10 USC – The Goldwater-Nichols Act
  - FY 14 National Defense Authorization Act – Section 932
- **Policy & Doctrine**
  - Presidential Policy Directive 20
  - National Security Presidential Directive-54
  - DoDI 8500.01 Cybersecurity
  - DoDI 8530.01 Cybersecurity Activities Support to DODIN Operations
  - DoDI 8510.01 Risk Management Framework (FMR) for DoD Information Technology
  - Joint Pub 3-12 cyberspace Operations
  - FM 3-38 Cyber Electromagnetic Activities
- **Directives, Regulations, & Orders**
  - DAGO 2014-02 ARCYBER as Army Force Component of USCYBERCOM and Second Army as DRU
  - AR 25-1 Army Information Technology
  - AR 25-2 Information Assurance (Cybersecurity)
  - AR 10-87 Army Commands, Army Service Component Commands and Direct Reporting Units

Cybersecurity Campaign

Recent Cyber Incidents





Most cyber attacks against DoD and others have exploited preventable vulnerabilities

DoD Cybersecurity Directives

- The *DoD Cybersecurity Campaign* identifies specific actions which drive commanders and DoD senior leaders to enforce full cybersecurity compliance and accountability
- Two campaign elements are *Cybersecurity Discipline Implementation Plan (CSDIP)* and the *DoD Cybersecurity Scorecard*

Scorecard Tasks	Goal
Ensure Every System Administrator Logs On via Public Key Infrastructure (PKI)*	95%
Ensure Every User Logs On via PKI	95%
Every Web Server on SIPRNet and Private Web Server on NIPRNet Must Use PKI for User Authentication	95%
Move all Outward-Facing Servers to Approved DMZs*	95%
Remove Windows XP Operating System Software from Entire SIPRNet & NIPRNet Inventory	99%
Remove Windows Server 2003 Operating System Software from Entire SIPRNet and NIPRNet Inventory	99%
Evaluate and Approve Systems, Fix Vulnerabilities, Perform Regular Security Control Testing	No weakness more than 120 days overdue
Implement Host-Based Security System	95%
Every Computer Properly Patched	95%
Every Computer Properly Configured	95%

* *DoD Near-term Priority Tasks*

95% – 100% | 75% – 94% | Below 75%

What is the Army doing

- **Established IPT to coordinate Army way-ahead**
- **Improving data accuracy**
- **Assessing system compliance**
- **Changing culture and behavior**

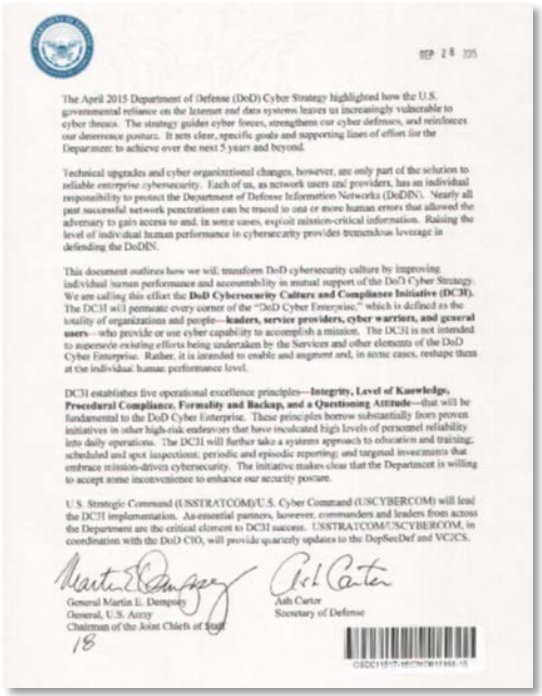
Conduct

- **Awareness**
- **Training**
  - Individual
  - Organizational
  - Annual
  - Periodic
- **Discipline**

5 Operational Excellence Principles

- Integrity
- Level of Knowledge
- Procedural Compliance
- Formality and Backup
- Questioning Attitude

DOD Cybersecurity Culture and Compliance initiative (DC3I)



The April 2015 Department of Defense (DoD) Cyber Strategy highlighted how the U.S. governmental reliance on the Internet and data systems leaves us increasingly vulnerable to cyber threats. The strategy guides cyber forces, strengthens our cyber defenses, and reinforces our deterrence posture. It sets clear, specific goals and supporting lines of effort for the Department to achieve over the next 5 years and beyond.

Technical upgrades and cyber organizational changes, however, are only part of the solution to reliable enterprise cybersecurity. Each of us, as network users and providers, has an individual responsibility to protect the Department of Defense Information Networks (DoDIN). Nearly all past successful network penetrations can be traced to one or more human errors that allowed the adversary to gain access to and, in some cases, exploit mission-critical information. Raising the level of individual human performance in cybersecurity provides tremendous leverage in defending the DoDIN.

This document outlines how we will transform DoD cybersecurity culture by improving individual human performance and accountability in mutual support of the DoD Cyber Strategy. We are calling this effort the **DoD Cybersecurity Culture and Compliance Initiative (DC3I)**. The DC3I will permeate every corner of the "DoD Cyber Enterprise," which is defined as the totality of organizations and people—**leaders, service providers, cyber warriors, and general users**—who provide or use cyber capability to accomplish a mission. The DC3I is not intended to supersede existing efforts being undertaken by the Services and other elements of the DoD Cyber Enterprise. Rather, it is intended to enable and augment and, in some cases, reshape them at the individual human performance level.

DC3I establishes five operational excellence principles—**Integrity, Level of Knowledge, Procedural Compliance, Formality and Backup, and a Questioning Attitude**—that will be fundamental to the DoD Cyber Enterprise. These principles borrow substantially from proven initiatives in other high-risk endeavors that have inculcated high levels of personnel reliability into daily operations. The DC3I will further take a systems approach to education and training; scheduled and spot inspections; periodic and episodic reporting; and targeted investments that embrace mission-driven cybersecurity. The initiative makes clear that the Department is willing to accept some inconvenience to enhance our security posture.

U.S. Strategic Command (USSTRATCOM)/U.S. Cyber Command (USCYBERCOM) will lead the DC3I implementation. As essential partners, however, commanders and leaders from across the Department are the critical element to DC3I success. USSTRATCOM/USCYBERCOM, in coordination with the DoD CIO, will provide quarterly updates to the DepSecDef and VCJCS.

General Martin E. Dempsey
General, U.S. Army
Chairman of the Joint Chiefs of Staff

Ash Carter
Secretary of Defense

Cybersecurity Awareness Month

October is Cybersecurity Awareness Month

- Third year of an Army-wide awareness effort
- Coincides with National Cyber Security Awareness Month
- Reinforces the DHS theme: *"Celebrating 5 Years of Stop. Think. Connect.™"*

- Focus on risk management and insider threat
- Build awareness of all Army leaders the need to assess and manage risks, conduct continuous monitoring practices to identify, assess and respond to vulnerabilities
- Creates a culture of awareness that anticipates, detects, and responds to insider threats before they can impact Army networks

Supports the Army's overall capability to continuously assess cyber operational readiness, security and reliability

Capability

Enterprise

- Web Content Filter (WCF)
- Access Control List (ACL)
- SHARKSEER
- (EEMSG)
- ECOS
- (ERS)
- Arbor
- .mil Proxy
- SSL Proxy

Enclave

- Web Application Filtering (WAF)
- DMZ
- DNSSEC
- HBSS

End Point

- HBSS AV
- HBSS ACCM
- HBSS DCM
- HBSS HIPS
- HBSS PA
- HBSS RSD
- EMET
- IAVM
- CMRS
- STIGS
- ACAS

Cyber Workforce

- **Workforce Roles**. Consensus on characterizing civilian cyberspace work roles.
- Matrix derived from DoD's implementation of NICE framework. Color-coding associates DCWF with three CF17 work role classification 'bins'. Parenthetical-coding reflects cross-walk of DCWF/CF17 association with DoDD 8140 cyberspace workforce areas.

Consolidated product associating work roles across three references provides foundation for determining training requirements for the civilian cyberspace workforce.

National Initiative for Cybersecurity Education (NICE)

DoD Cyberspace Workforce Framework (DCWF)

Category	Specialty Areas						
Securely Provision	Risk Management (CS)	Software Development (CIT)	Architecture (CIT)	Technology Research & Development (CIT)	Systems Requirements Planning (CIT)	Test and Evaluation (CIT)	Systems Development (CIT)
Operate & Maintain	Data Administration (CIT)	Knowledge Management (CIT)	Customer Service & Tech Support (CIT)	Network Services (CS)	System Administration (CS)	Systems Security Analysis (CS)	
Oversight & Development	Legal Advocacy & Advice (CS)	Education & Training (CS)	Cybersecurity Management (CS)	Strategic Planning & Policy (CS)	Acquisition and Program/Project Management (CS)	Executive Cyberspace Leadership (I/CE/CS)	
Protect & Defend	CND Analysis * (CE/CS)	CND Infrastructure Support * (CE/CS)	Incident Response (CS)	Vulnerability Assessment & Management (CS)			
Analyze	Threat Analysis (I)	Exploitation Analysis ** (I/CE)	All-Source Analysis (I)	Targets (I)			
Operate & Collect	Collection Operations (I)	Cyber Operational Planning ** (I/CE)	Cyber Operations ** (CE)				
Investigate	Investigation (CS)	Digital Forensics (CS)					

Color-coding: *Specialty Areas* contain associated work roles that cross-walk to *CF17 work roles:*
RED, to Core CF17 work roles
BLUE, to Direct Support CF17 work roles, and
GREEN, to Specialized Support CF17 work roles

Parenthetical-coding: *Specialty Areas* contain associated work roles that crosswalk to DoDD 8140 cyberspace workforce areas:
(CS), Cybersecurity (CE), Cyberspace Effects
(CIT), Cyberspace IT (I), Intelligence Workforce (Cyberspace)

* Primarily Career Program 34, Information Technology Management ** Primarily Career Program 35, Intelligence and Security

Civilian Cyberspace Workforce OPT- Overview

Goal: To unify the management of the Army civilian cyberspace workforce.

Objectives:

- Establish an Army enterprise methodology to clearly designate, recruit, develop, credential and retain the civilian cyberspace workforce.
- Develop a training pipeline with viable career management solutions to prepare a cadre of trained civilians to enter cyberspace work roles over the course of their careers.
- Implement best practices for recruiting, developing and retaining the civilian cyberspace workforce across the Army and DoD.

2210 IT Management (CP-34)
0391 Telecommunications (CP-34)

0855 Electronics Engineer (CP-16)
0854 Computer Engineer (CP-16)
1550 Computer Scientist (CP-16)

22100132 Intelligence Ops (CP-35)
22110080 Security Adm (CP-35/CP-19)
22121811 Criminal Investigation (CP-19)

1515 Ops Research (CP-36/CP-11)

*Derived from December 2014 OPM memorandum extending use of Schedule A Authority

Final Thoughts…

Stay Connected!

Unified Cybersecurity

CIOG6.ARMY.MIL

CIO/G-6

ENABLING SUCCESS

For Today and Tomorrow

Ms. Essye Miller

Director, Cybersecurity Army CIO/G-6

October 15, 2015