

16th ICCRTS

“Collective C2 in Multinational Civil-Military Operations”

Cyber Security to the Edge: Applying Edge Theory to Cyber Security Operations

Topics

Topic 11: Cyberspace Management

Topic 2: Approaches and Organizations

Topic 5: Collaboration, Shared Awareness, and Decision Making

Name of Author

Chris Simpson

San Diego, CA

Point of Contact

Chris Simpson

Independent Researcher

Telephone: 619-865-7294

Email: csimpson4@mac.com

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Cyber Security to the Edge: Applying Edge Theory to Cyber Security Operations			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Chris Simpson,Independent Researcher,San Deigo,CA,92126			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.					
14. ABSTRACT Defending Department of Defense networks is a complex endeavor. Our current method of defending networks starts with topdown rules, policies and regulations. These rules and regula-tions are complex and in many cases may be redundant or contradicted to meet an urgent opera-tional requirement. Additionally the requirements contained in these policies are not always funded. This paper will examine if edge organizational techniques and Edge Theory could be applied to cyber security organizations to improve the defense of DoD networks.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 24	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Abstract

Defending Department of Defense networks is a complex endeavor. Our current method of defending networks starts with topdown rules, policies and regulations. These rules and regulations are complex and in many cases may be redundant or contradicted to meet an urgent operational requirement. Additionally the requirements contained in these policies are not always funded. This paper will examine if edge organizational techniques and Edge Theory could be applied to cyber security organizations to improve the defense of DoD networks.

Introduction

Defending Department of Defense networks is a complex endeavor with an extensive amount of topdown rules, policies and regulations. These rules and regulations are complex and in many cases may be redundant or contradicted to meet an urgent operational requirement. In some cases new rules are created across the enterprise in response to a specific event at one part of the organization (i.e. Wiki leaks) without much thought to the impact on the entire organization. Additionally the requirements contained in these policies are not always funded. DoD networks could be better defended by organizing as an edge organization. This paper will introduce this concept and start the discussion to examine if edge organizational techniques and edge theory could be applied to cyber security organizations to improve the defense of DoD networks.

Edge Theory

In order to understand why an Edge organization will improve the performance of a cyber security organization we must have a common definition of an Edge organization and understand the characteristics of an Edge organization. Alberts defines an Edge organization as “Edge organizations are organizations where everyone is empowered by information and has the freedom to do what makes sense” [1]. Members in an Edge organization members are empowered to share information and most relationships are of a peer-to-peer nature. This eliminates the distinction between line and support personnel as well as the associated stovepipes of that artificial division. By flattening an organization the requirement for the “middle” part of an organization that relays communications within that organization is greatly reduced. This reduction of the “middle” and stovepipes removes “barriers to information sharing and collaboration” within that organization and between the components of that organization [1].

Current Top Down Structure

Under our current cyber structure senior leadership develops high level and detailed policy guidance along with extensive reporting requirements. The DoD Information Assurance Technology Analysis Center has a chart (Figure 1) that displays all of the guidance required to “Build and Operate a Trusted GIG” [2].

security official, Robert Lentz, said the Defense Department detected 360 million attempts to penetrate its networks last year, up from six million in 2006“ [3].

With such a high number of attacks how can a hierarchical and centralized organization manage the response to so many attempted attacks? “Cyberwarfare is like maneuver warfare, in that speed and agility matter most”[4]. By moving to an edge cyber security organization and allowing action at the edge make it easier to defend and respond to cyber attacks.

The Fog of War in Cyber Warfare

Information overload is one of the major factors for “fog of war” in cyber warfare. If every organization followed the current rules they would conduct recurring vulnerability scans and this data would be fed into different databases so the chain of command would have a list of 1000’s of vulnerabilities but does this enhance the overall security of the scanned systems if the owners don’t have the tools or manpower to resolve those vulnerabilities? With the amount and complexity of this data there is no way for a centralized organization make sense of this. This is analogous to telling Platoon commander to defend a street block but instead of letting him deploy his troops he would first have to scan the block for vulnerabilities on a checklist and submit those vulnerabilities to higher HQ. Many of the vulnerabilities on the checklist might not be applicable to the current situation, higher headquarters would asses the listed vulnerabilities them and tell the Platoon Commander which ones to fix. As this data makes its way up the chain of command the enemy disposition is constantly changing and by the time a response is received from upper echelon it may be too late to defend the block. Instead of doing this the Army develops tactics, techniques and procedures (TTPs) for the Platoon Commander to utilize that can be modified based on the local situation.

The attacker has the advantage in cyber warfare, the attacker only needs to know one vulnerability to gain access to a system while the defender must monitor all vulnerabilities. This advantage is increased when a defender operates in a hierarchical organization and must wait for top down direction to take action. Local units defending their own networks would have a smaller footprint and less data to monitor making it easier to detect attacks.

Cyber Warfare Command and Control

Even in an edge organization leadership must be involved in setting overall guidance and have situational awareness to the overall health of their systems. Under current vulnerability system the status individual systems are reported up the chain of command. A commander doesn’t need to know the exact status of each system, rather he needs to know the impact of those vulnerabilities. In an edge organization the commander would establish high level goals and requirements. A good example of establishing high level guidance is the “Ten Things Every Airman

Must Know in the United States Air Force Doctrine Document 3-12 of 15 July 2010 “Cyber-space Operations”:

1. The United States is vulnerable to cyberspace attacks by relentless adversaries attempting to infiltrate our networks at work and at home – millions of times a day, 24/7.
2. Our enemies plant malicious code, worms, botnets, and hooks in common websites, software, and hardware such as thumbdrives, printers, etc.
3. Once implanted, this code begins to distort, destroy, and manipulate information, or —phone it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.
4. The enemy attacks your computers at work and at home knowing you communicate with the Air Force network by email, or transfer information from one system to another.
5. As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates, and your country.
6. You significantly decrease our enemies’ access to our networks, critical USAF information, and even your personal identity by taking simple action.
7. Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.
8. Do not connect any hardware or download any software applications, music, or information onto our networks without approval
9. Encrypt sensitive but unclassified and/or critical information. Ask your computer systems administrator (CSA) for more information
10. Install the free Department of Defense anti-virus software on your home computer. Your CSA can provide you with your free copy” [5].

This guidance is easy to understand and implement. One can boil down the current policy to some similarly simply stated goals that could be implemented in an edge Organization:

1. Resilient network and information systemsBuild resilience at local level
2. Design secure systems from the start
3. Secure your system from current known vulnerabilities and monitor for attacks on open vulnerabilities
4. Monitor your system
5. Correlate attacks to known vulnerabilities
6. Respond to attacks
7. Communicate with higher headquarters

(Author’s interpretation of guidance listed on IATC 2011 [2])

Creating an Edge Cyber Security Organization

In order to become an edge cyber security organization we should consider locations as nodes on a network and empower those nodes to defend themselves and their neighbors. The term neighbors is used in the relationship between nodes on a network not their physical location. The first step would be to identify the policy that enhances cyber security, for example manning requirements to defend a local enclave. The next step can be done by providing pre built templates like the current Defense Information System Agency Gold Disk templates for

common functions and let them develop defense for their unique systems. These nodes would also need visibility into their local network traffic and tools to assess their local vulnerabilities. There are already a variety of tools in use by the DOD that can accomplish this. They would also communicate with their neighbors and gain value by some type of mutual defense. To test the effectiveness of an edge organization a test enclave could be established that is empowered to defend their own network and communicate directly with anyone along their network path. Although a detailed test would have to be developed, below are some areas that could be measured to see the effectiveness of an edge organization [6]:

Quality of organic information

- Awareness of what is on the enclave
- Awareness of attacks (successful and unsuccessful)
- Awareness of vulnerabilities

Quality of organic Information

Quality of Individual Sense making

- Do the operators understand what is on their network

Quality of interactions

Degree of shared information

Extent: Measure flow of information from enclave to neighboring enclaves, CND service providers, and higher HQ. This could be measured by: exchange of correlating IDS alerts, exchange of vulnerability alerts and status of connected systems (i.e. Vulnerabilities, accepted risk) [6].

The data collected from this test could be compared with similar data from other enclaves to see if there was an improvement in overall security

In many cases a cyber security event in one node can impact another node or have a broader impact to the organization. Systems that have any possibility of impacting outside of a node or that can have a broader impact on the enterprise would have to be identified and specific reporting requirements would have to be developed to notify the chain of command with appropriate time reporting requirements. This could be accomplished in many ways including the use of auto-reporting network sensors. Some examples of automatic external reporting requirements:

- Public exposure of sensitive or classified data

- Identification of self replicating worm
- Insider attack from one node to another

It is difficult for non security experts to understand the current way security incidents are handled. To better illustrate this the story below applies the methods we use to respond to computer attacks to the Navy Medical system.

Applying the Current Cyber Defense Workflow to the Medical System

Seaman Timmy (compromised computer) assigned to a ship catches the flu. The Navy Medical Command (Service Computer Emergency Response Team) in Bethesda, MD sends the corpsman on the ship an alert (intrusion detection alerts) that someone, but not a specific person, is sick and that he needs to be isolated immediately. The corpsman must search the ship to find the sick Sailor. Once found the corpsman must contact the medical command and receive guidance on how to aid Seaman Timmy. If the corpsman doesn't answer all questions there may be additional questions. The Medical Command's directive to isolate Seaman Timmy may endanger the ship since Seaman Timmy is the helmsman, steering the ship while at sea, (critical system). Once all of the information has been received by the medical command they will tell the corpsman to respond. Let's say the diagnosis is a bacterial infection the medical command may prescribe an antibiotic. Since they don't have access to Seaman Timmy's medical record (DI-ACAP package) they may not know he is allergic to antibiotics putting him at risk.

How would an edge organization better handle the response to a computer attack? First a local sensor or other cueing detects compromised host. Local network defender locates system and determines criticality of the system. Since they know the most about the system they can take the best steps to immediately isolate that system with the least impact. The local defenders would also know the system's relationship and possible impact to connected systems and could alert adjacent system defenders as appropriate.

Conclusion

Defending the global information grid against attacks from Nation States, individual hackers, organized crime and malicious insiders is a complex task and problem. Solving complex problems requires innovative solutions that push down responsibility and empower people at the local level to defend their networks and systems. Self organized groups of defenders in an edge organization offers many advantages to the current top down hierarchical structure. These advantages include quicker response to network attacks by empowering individuals at the unit level, resilient networks by improving information sharing and reducing the administrative burden by removing redundant policy and flattening the cyber security organization. Higher echelons would have better situational awareness because they could focus on information from the edge that has been identified as critical rather than sifting through huge amounts of data reports without context.

References

- [1] Alberts, D.S. and Hayes, R.E. (2003). *Power to the Edge*. Washington, DC: CCRP.
- [2] Build and Operate a Trusted GIG. (2011). [Cyber, Identity & Information Assurance (CIIA) Related Policies and Issuances]. Information Assurance Technology Analysis Center. Retrieved from: http://iac.dtic.mil/iatac/download/ia_policychart.pdf
- [3] Dreazen, Y.J. And Gorman, S. (6 May 2009). U.S. Cyber Infrastructure Vulnerable to Attacks. *Wall Street Journal*. Retrieved from <http://online.wsj.com/article/SB124153427633287573.html>
- [4] Lynn, William. (2010). Defending a New Domain: the Pentagon's Cyberstrategy. U.S. Department of Defense. Retrieved from http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx
- [5] United States Air Force (USAF). (2010). *Cyberspace Operations* (Air Force Doctrine Document 3-12). Retrieved from <http://www.airforce-magazine.com/SiteCollectionDocuments/TheDocumentFile/Strategy%20and%20Concepts/AFDD3-12.pdf>
- [6] Office of Force Transformation. (2003). Network Centric Operations Conceptual Framework Version 1.0. Vienna, VA: Evidence Based Research.

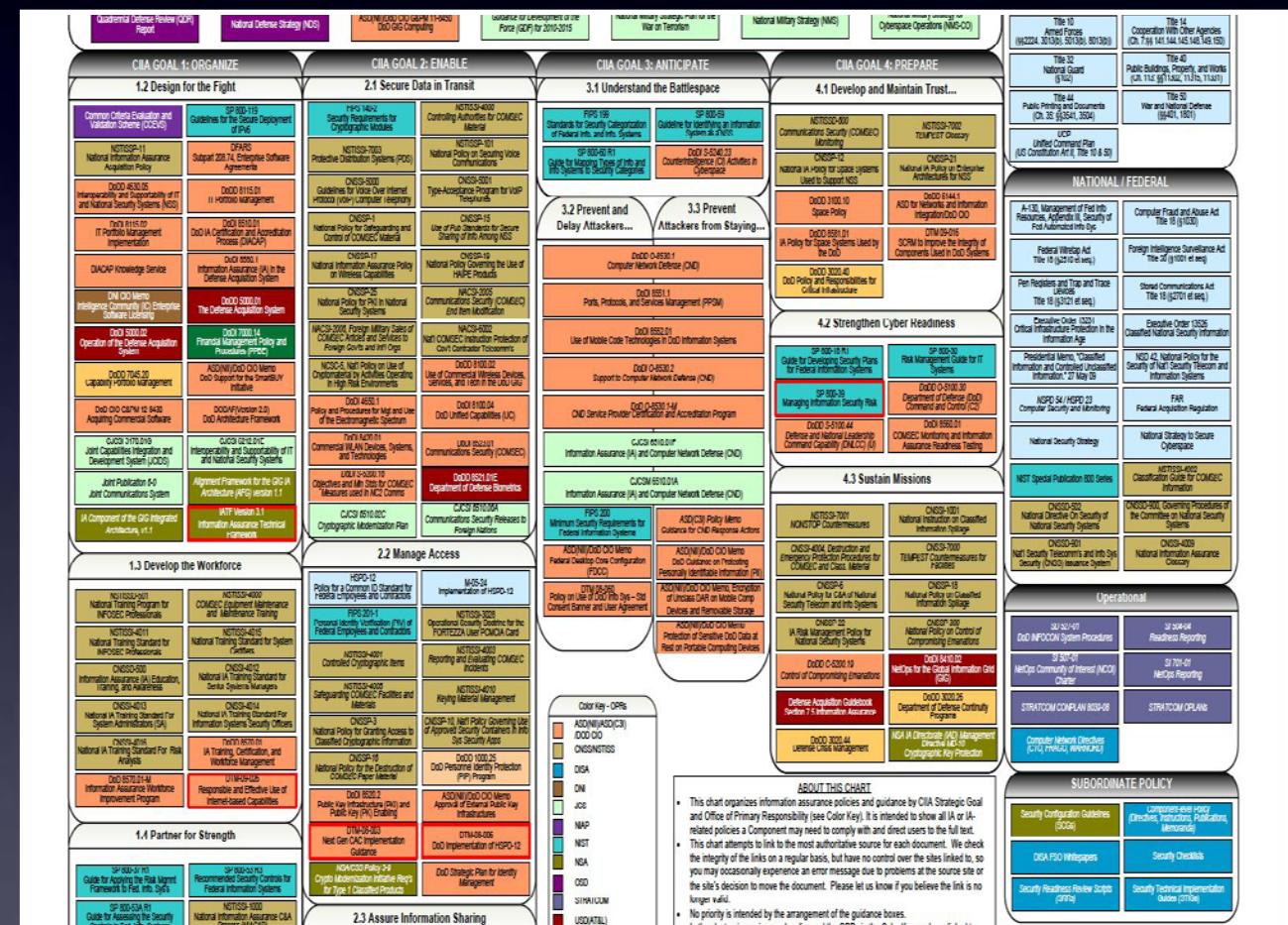
Cyber Security to the Edge

Applying Edge Theory to Cyber Security Operations

Chris Simpson

Defending DoD Networks

- Top Down Approach
- Complex
- Rules to meet urgent requirements or specific events



Top Down Structure

- “Abundance” of guidance
- Certification and Accreditation process versus real security
- Centralized planning versus agile hackers

Build and Operate a Trusted GIG

Cyber, Identity & Information Assurance (CIIA)

Related Policies and Issuances

Developed by DASD(CIIA)

Last Updated: April 4, 2011

Send questions/suggestions to iatac@dtic.mil

CIIA GOAL 1: ORGANIZE

1.1 Lead and Govern

25 Point Implementation Plan to Reform Federal IT Mgt.	Cyberspace Policy Review	CNSCSP 34 Policy on Assured Info Sharing (AIS) for National Security Systems (NSS)	DoDD 8000.01 Management of the DoD Information Enterprise	DoDD 8500.01E Information Assurance (IA)	DoDI 8500.2 Information Assurance Implementation	DoD Cyber, Identity & Information Assurance Strategic Plan
Quadrennial Defense Review (QDR) Report	National Defense Strategy (NDS)	ASD(NII)/DoD CIO G&PM 11-5450 DoD GIG Computing	Guidance for Development of the Force (GDF) for 2010-2015	National Military Strategic Plan for the War on Terrorism	National Military Strategy (NMS)	National Military Strategy for Cyberspace Operations (NMS-CO)

CIIA GOAL 1: ORGANIZE

1.2 Design for the Fight

Common Criteria Evaluation and Validation Scheme (CCEVS)	SP 800-119 Guidelines for the Secure Deployment of IPv6
NSTISSP-11 National Information Assurance Acquisition Policy	DFARS Subpart 208.74, Enterprise Software Agreements
DoDD 4630.05 Interoperability and Supportability of IT and National Security Systems (NSS)	DoDD 8115.01 IT Portfolio Management
DoDI 8115.02 IT Portfolio Management Implementation	DoDI 8510.01 DoD IA Certification and Accreditation Process (DIACAP)
DIACAP Knowledge Service	DoDI 8500.1 Information Assurance (IA) in the Defense Acquisition System
ONI CIO Memo Intelligence Community (IC) Enterprise Software Licensing	DoDD 5000.01 The Defense Acquisition System
DoDI 5000.02 Operation of the Defense Acquisition System	DoDI 7000.14 Financial Management Policy and Procedures (PPRIS)
DoDD 7045.20 Capability Portfolio Management	ASD(NII)/DoD CIO Memo DoD Support for the SmartBUY Initiative
DoDD CIO G&PM 12-5430 Acquiring Commercial Software	DoDAF (Version 2.0) DoD Architecture Framework
CJCSI 3170.01G Joint Capabilities Integration and Development System (JCIDS)	CJCSI 6312.01E Interoperability and Supportability of IT and National Security Systems
Joint Publication 6-0 Joint Communications System	Alignment Framework for the GIG IA Architecture (AFIC) version 1.1
IA Component of the GIG Integrated Architecture, v1.1	IATF Version 3.1 Information Assurance Technical Framework

1.3 Develop the Workforce

NSTISSP-501 National Training Program for INFOSEC Professionals	NSTISSP-4000 COMSEC Equipment Maintenance and Maintenance Training
NSTISSP-4011 National Training Standards for INFOSEC Professionals	NSTISSP-4015 National Training Standards for System Centers
CNSCSP-300 Information Assurance (IA) Education, Training, and Awareness	CNSCSP-4012 National IA Training Standard for Senior Systems Managers
CNSCSP-4013 National IA Training Standard for System Administrators (SA)	CNSCSP-4014 National IA Training Standard for Information Systems Security Officers
CNSCSP-4016 National IA Training Standard For Risk Analysts	DoDD 8570.01 IA Training, Certification, and Workforce Management
DoD 8570.01-M Information Assurance Workforce Improvement Program	DTM-09-005 Responsible and Effective Use of Internet-based Capabilities

1.4 Partner for Strength

SP 800-37 R1 Guide for Applying the Risk Mgmt Framework to Fed. Info. Sys's	SP 800-53 R3 Recommended Security Controls for Federal Information Systems
SP 800-53A R1 Guide for Assessing the Security Controls in Fed. Info. Systems	NSTISSP-1000 National Information Assurance C&A Process (NIACAP)
CNSCSP-1253 Security Categorization and Control Selection for Nat'l Security Systems	CNSCSP-4007 Communications Security (COMSEC) Utility Program
CNSCSP-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment	CNSCSP-14 National Policy Governing the Release of IA Products/Services
DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities	ISO 9001 IT Systems Security Risk Management and C&A

CIIA GOAL 2: ENABLE

2.1 Secure Data in Transit

FIPS 140-2 Security Requirements for Cryptographic Modules	NGTSSP-4000 Controlling Authorities for COMSEC Material
NGTSSP-7003 Protective Distribution Systems (PDS)	NGTSSP-101 National Policy on Securing Voice Communications
CNSCSP-5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony	CNSCSP-3001 Type-Acceptance Program for VoIP Telephones
CNSCSP-1 National Policy for Safeguarding and Control of COMSEC Material	CNSCSP-15 Use of Pub. Standards for Secure Sharing of Info Among NSS
CNSCSP-17 National Information Assurance Policy on Wireless Capabilities	CNSCSP-19 National Policy Governing the Use of HAPPE Products
CNSCSP-25 National Policy for PKI in National Security Systems	NACSS-2005 Communications Security (COMSEC) End Item Modification
NACSS-2000, Foreign Military Sales of COMSEC Articles and Services to Foreign Govts and Int'l Orgs	NACSS-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomms
NCSIC-5, Nat'l Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments	DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
DoDI 4600.1 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum	DoDI 8100.04 DoD Unified Capabilities (UC)
DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies	DoDI 8523.01 Communications Security (COMSEC)
DoDI 8520.10 Objectives and Min Stds for COMSEC Measures used in NC2 Comms	DoDD 8521.01E Department of Defense Biometrics
CJCSI 6510.02C Cryptographic Modernization Plan	CJCSI 6510.05A Communications Security Released to Foreign Nations

2.2 Manage Access

HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors	M-05-24 Implementation of HSPD-12
FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors	NSTISSP-3028 Operational Security Doctrine for the FORTEZZA User POMCIA Card
NSTISSP-4001 Controlled Cryptographic Items	NSTISSP-4003 Reporting and Evaluating COMSEC Incidents
NSTISSP-4005 Safeguarding COMSEC Facilities and Materials	NSTISSP-4010 Keying Material Management
CNSCSP-3 National Policy for Granting Access to Classified Cryptographic Information	CNSCSP-10, Nat'l Policy Governing Use of Approved Security Containers & Info Sys Security Apps
CNSCSP-15 National Policy for the Destruction of COMSEC Paper Material	DoDD 1000.25 DoD Personnel Identity Protection (PIP) Program
DoDI 8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	ASD(NII)/DoD CIO Memo Approval of External Public Key Infrastructures
DTM-08-003 Next Gen CAC Implementation Guidance	DTM-08-006 DoD Implementation of HSPD-12
NSA/CSS Policy 3-9 Crypto Modernization Initiative Req's for Type 1 Classified Products	DoD Strategic Plan for Identity Management

2.3 Assure Information Sharing

DoDD 8320.02 Data-Sharing in a Net-Centric Department of Defense	United States Intelligence Community Information Sharing Strategy
ASD(NII)/DoD CIO Memo Use of Peer-to-Peer File Sharing Applications Across DoD	DTM-08-027 Security of Unclassified DoD Information on Non-DoD Info Systems
DoD Information Sharing Strategy	Cross Domain Community Roadmap
CJCSI 6211.02C Defense Information System Network Policy and Responsibilities	CJCSM 3213.02C Joint Staff Focus Point

CIIA GOAL 3: ANTICIPATE

3.1 Understand the Battlespace

FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems	SP 800-59 Guideline for Identifying an Information System as a NSS
SP 800-60 R1 Guide for Mapping Types of Info and Info Systems to Security Categories	DoDI 8524.01 Counterintelligence (CI) Activities in Cyberspace

3.2 Prevent and Delay Attackers...

3.3 Prevent Attackers from Staying...

DoDD O-8530.1 Computer Network Defense (CND)	DoDI 8551.1 Ports, Protocols, and Services Management (PPSM)
DoDI 8552.01 Use of Mobile Code Technologies in DoD Information Systems	DoDI 8552.01 Support to Computer Network Defense (CND)
DoDD O-8530.2 Support to Computer Network Defense (CND)	DoDD O-8530.1-M CND Service Provider Certification and Accreditation Program
CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)	CJCSM 6510.01A Information Assurance (IA) and Computer Network Defense (CND)
FIPS 200 Minimum Security Requirements for Federal Information Systems	ASD(C3) Policy Memo Guidance for CND Response Actions
ASD(NII)/DoD CIO Memo Federal Desktop Core Configuration (FDCC)	ASD(NII)/DoD CIO Memo DoD Guidance on Protecting Personally Identifiable Information (PII)
DoDI 8550.01 Policy on Use of DoD Info Sys - Std Consent Banner and User Agreement	ASD(NII)/DoD CIO Memo Encryption of Unclassified Data on Mobile Comp Devices and Removable Storage
	ASD(NII)/DoD CIO Memo Protection of Sensitive DoD Data at Rest on Portable Computing Devices

Color Key - OPRs
ASD(NII)/DoD(C3)/DoD CIO
CNSCSP/STISS
DISA
ONI
JCS
NIAP
NIST
NSA
OSD
STRATCOM
USO(AT&L)
USO(C)
USO(I)
USO(P)
USO(P&R)
Other Agencies
Recently updated box

ABOUT THIS CHART

- This chart organizes information assurance policies and guidance by CIIA Strategic Goal and Office of Primary Responsibility (see Color Key). It is intended to show all IA or IA-related policies a Component may need to comply with and direct users to the full text.
- This chart attempts to link to the most authoritative source for each document. We check the integrity of the links on a regular basis, but have no control over the sites linked to, so you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- No priority is intended by the arrangement of the guidance boxes.
- In the electronic version, each policy and the OPRs in the Color Key are hyperlinked to their full text or respective sites online. To use the hyperlink, simply click on the box.
- Policies in italics indicate the document is marked for limited distribution or no public-facing hyperlink is currently available.
- Boxes with red borders reflect recent updates.
- For printing, this chart is best viewed on 22"x17" (Size C) paper.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than \$1.00.
- For the latest version of this chart go to http://iac.dtic.mil/iatac/ia_policychart.html.

AUTHORITIES

Clinger-Cohen Act, Pub. L. 104-106	Federal Information Security Management Act, 44 U.S.C. §3541 et seq
Title 10 Armed Forces (§§2224, 3013(e), 5013(b), 6013(b))	Title 14 Cooperation With Other Agencies (Ch. 7 §§ 141, 144, 145, 148, 149, 150)
Title 32 National Guard (§ 102)	Title 40 Public Buildings, Property, and Works (Ch. 113: §§ 11302, 11315, 11331)
Title 44 Public Printing and Documents (Ch. 35: §§3541, 3504)	Title 50 War and National Defense (§§401, 1801)
UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)	

NATIONAL / FEDERAL

A-130, Management of Fed Info Resources, Appendix II, Security of Fed Automated Info Sys	Computer Fraud and Abuse Act Title 18 (§1030)
Federal Wiretap Act Title 18 (§2510 et seq.)	Foreign Intelligence Surveillance Act Title 50 (§1501 et seq.)
Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)	Stored Communications Act Title 18 (§2701 et seq.)
Executive Order 13331 Critical Infrastructure Protection in the Information Age	Executive Order 13526 Classified National Security Information
Presidential Memo, "Classified Information and Controlled Unclassified Information," 27 May 09	NSA 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
NSP 54 / HSPD 23 Computer Security and Monitoring	FAR Federal Acquisition Regulation
National Security Strategy	National Strategy to Secure Cyberspace
NIST Special Publication 800 Series	NSTISSP-4002 Classification Guide for COMSEC Information
CNSCSP-502 National Directive on Security of National Security Systems	CNSCSP-900, Governing Procedures of the Committee on National Security Systems
CNSCSP-901 Nat'l Security Telecoms and Info Sys Security (CNSCSP) Issuance System	CNSCSP-4009 National Information Assurance Glossary

Operational

SI 504-04 DoD INFOCOM System Procedures	SI 504-04 Readiness Reporting
SI 507-01 NetOps Community of Interest (NCOI) Charter	SI 701-01 NetOps Reporting
STRATCOM CONPLAN 8030-08	STRATCOM OPLANs
Computer Network Devices (CND, FRAGO, WARNORD)	

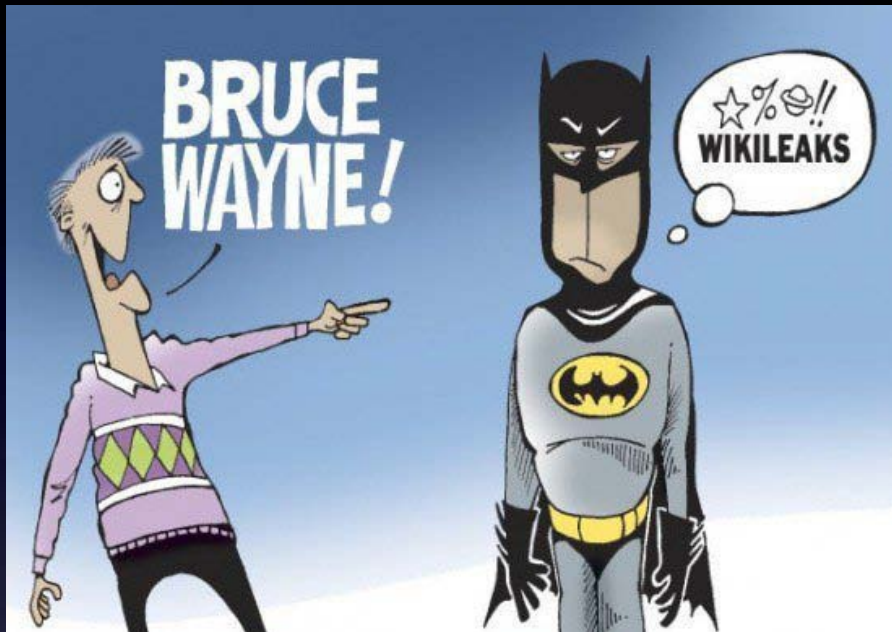
SUBORDINATE POLICY

Security Configuration Guidelines (SCGs)	Component-level Policy (Directives, Instructions, Publications, Memoranda)
DISA P50 Whitepapers	Security Checklists
Security Readiness Review Scripts (SRRS)	Security Technical Implementation Guides (STIGs)

Complex Systems

- Configuration options
- Locations around the world and rapid deployments
- Limited infrastructure support
- Competing interests and requirements
 - Services, mission etc
- Procurement cycle

Emergent Rules



BBC NEWS | South Asia | Afghans selling US army 'files'

http://news.bbc.co.uk/2/hi/south_asia/4905052.stm

Apple dashkards Kids Search SCO0275 - Jamis sdnifosec SDinfosec Manager lynda.com Diigolet Eason Des

Home News Sport Radio TV Weather Languages

an error occurred while processing this directive]

Low graphics | Accessibility help

BBC NEWS

Watch One-Minute World News

Last Updated: Wednesday, 12 April 2006, 23:07 GMT 00:07 UK

E-mail this to a friend Printable version

Afghans selling US army 'files'

US forces in Afghanistan are checking reports that stolen computer hardware containing military secrets is being sold at a market beside a big US base.

Shopkeepers at a market next to Bagram base, outside Kabul, have been selling memory drives stolen from the facility, the Los Angeles Times newspaper says.

The disks reportedly contain personal details about US soldiers, military defences and lists of enemy targets.

A US spokesman said an investigation had been ordered into the reports.

Lt Mike Cody said the military was looking into "allegations that sensitive military items are being sold in local bazaars".

AFGHANISTAN'S FUTURE FEATURES AND ANALYSIS

Regional focus
New Obama strategy puts spotlight on reconstruction

- Fortress Kabul
- Pakistan pessimism
- Changing times
- Out of favour
- Twenty-year war
- Winter hardship
- Driven apart

BACKGROUND

- In graphics: Life in Afghanistan
- Quick guide: Afghanistan
- Who are the Taliban?
- Q&A: Isaf troops explained

VIDEO AND AUDIO

- Watch Afghanistan's looming food crisis
- Watch Three summers in Afghanistan

SERVICES

Also in the news

- Video and Audio
- Programmes
- Have Your Say
- In Pictures
- Country Profiles
- Special Reports

DoD BUZZ
ONLINE DEFENSE AND ACQUISITION JOURNAL

Home Land Naval Air Commentary Space Cyber Security Intelligence

ADVERTISEMENT

UMUC CYBERSECURITY

> CYBER WARRIORS WANTED. > ENR

> BACHELOR'S, MASTER'S AND GRADUATE CERTIFICATES.

University of Maryland

DoD BUZZ SPECIAL SECTION

CYBER SECURITY
and Procurement of Security Systems

PRESENTED BY University of Maryland University College

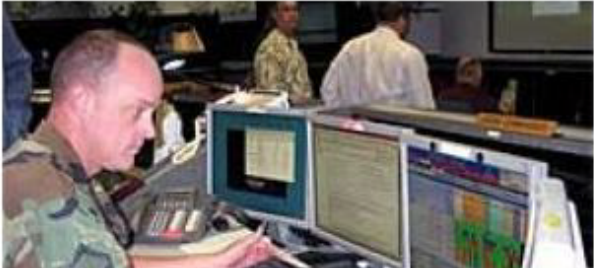
Home » Cyber Security » Cyber Attack Spurs Thumb Drive Ban

Cyber Attack Spurs Thumb Drive Ban

By Colin Clark Friday, November 21st, 2008 3:22 pm
Posted in Cyber Security, Policy

Like 3 people like this. Be the first of your friends.

Our friends at DefenseTech.org feature an excellent piece about a cyber attack on the U.S. military. The attack finally led to the military banning thumb drives and other portable memory tools from use on military networks.



Edge Theory

- Empowered individuals
- Removal of collaboration barriers

Fog of War in Cyber Warfare

- Information Overload
- Attacker advantage
- Platoon analogy

How would it work?

Cyber Warfare C2

- Keep high level guidance simple
- “Ten Things Every Airman Must Know”
- “Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source—even if it appears to be from someone you know.”

- United States Air Force (USAF). (2010). Cyberspace Operations

Keeping It Simple

- Resilient network and information systems, build resilience at local level
- Design secure systems from the start
- Secure your system from current known vulnerabilities and monitor for attacks on open vulnerabilities
- Monitor your system
- Correlate attacks to known vulnerabilities
- Respond to attacks
- Communicate with higher headquarters

An Edge Like Cyber Security Organization Organization

- Identify policy that enhances security, dump the rest
- Use templates like Gold Disk and encourage collaboration and sharing of these (i.e. same IT requirements)
- Provide local network visibility
- Treat CND service providers as sensors to support local enclaves
- Use IA Workforce

Measuring Success

- Quality of organic information
 - ✓ Awareness of what is on the enclave
 - ✓ Awareness of attacks
 - ✓ Awareness of vulnerabilities
- Quality of Individual Sense Making
 - ✓ What do the operators know
- Quality of interactions
 - ✓ Degree of shared information

Cyber Defense Workflow Example

Questions?

csimpson4@mac.com