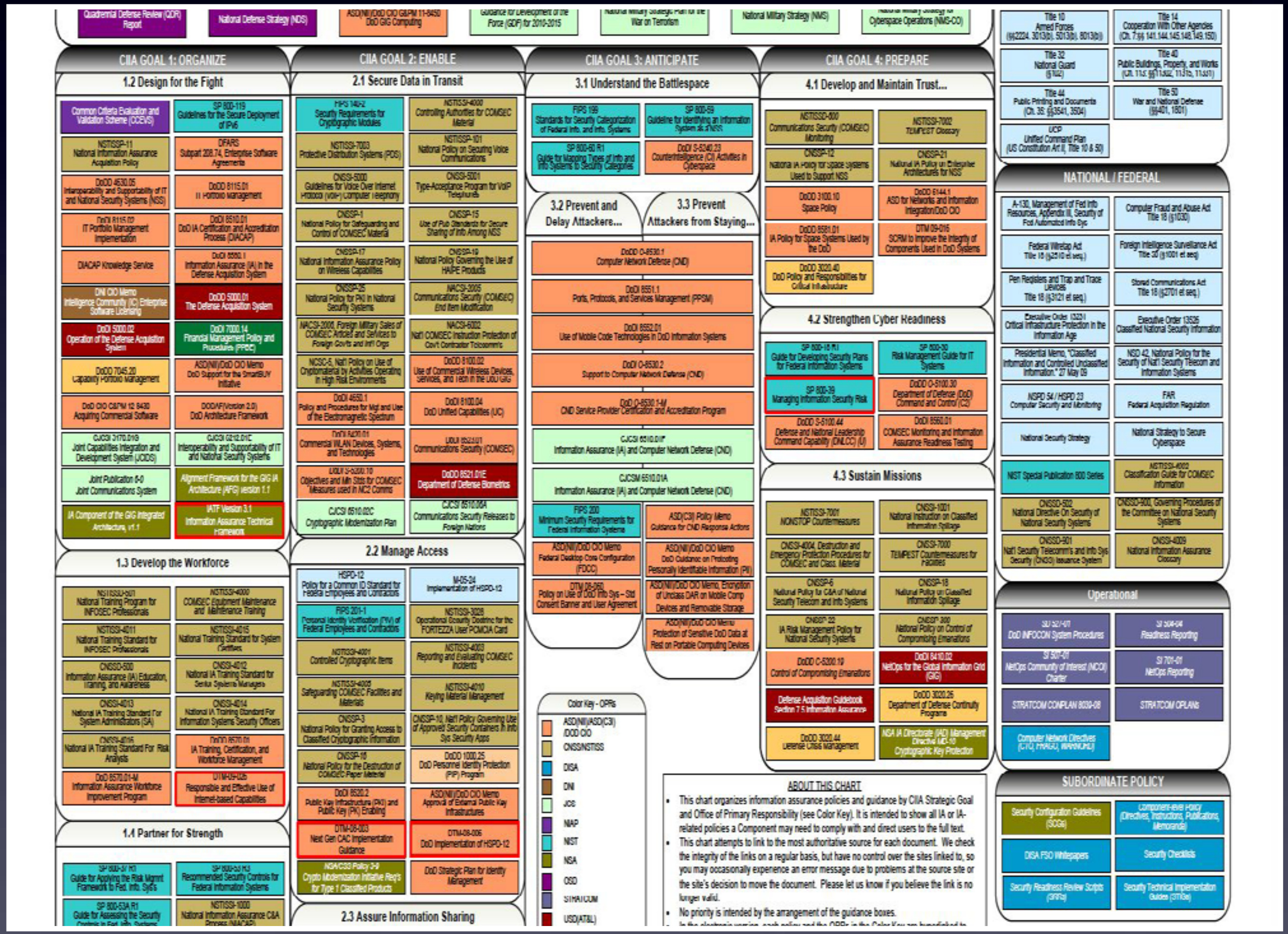
Cyber Security to the Edge

Applying Edge Theory to Cyber Security Operations

Chris Simpson

Defending DoD Networks

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

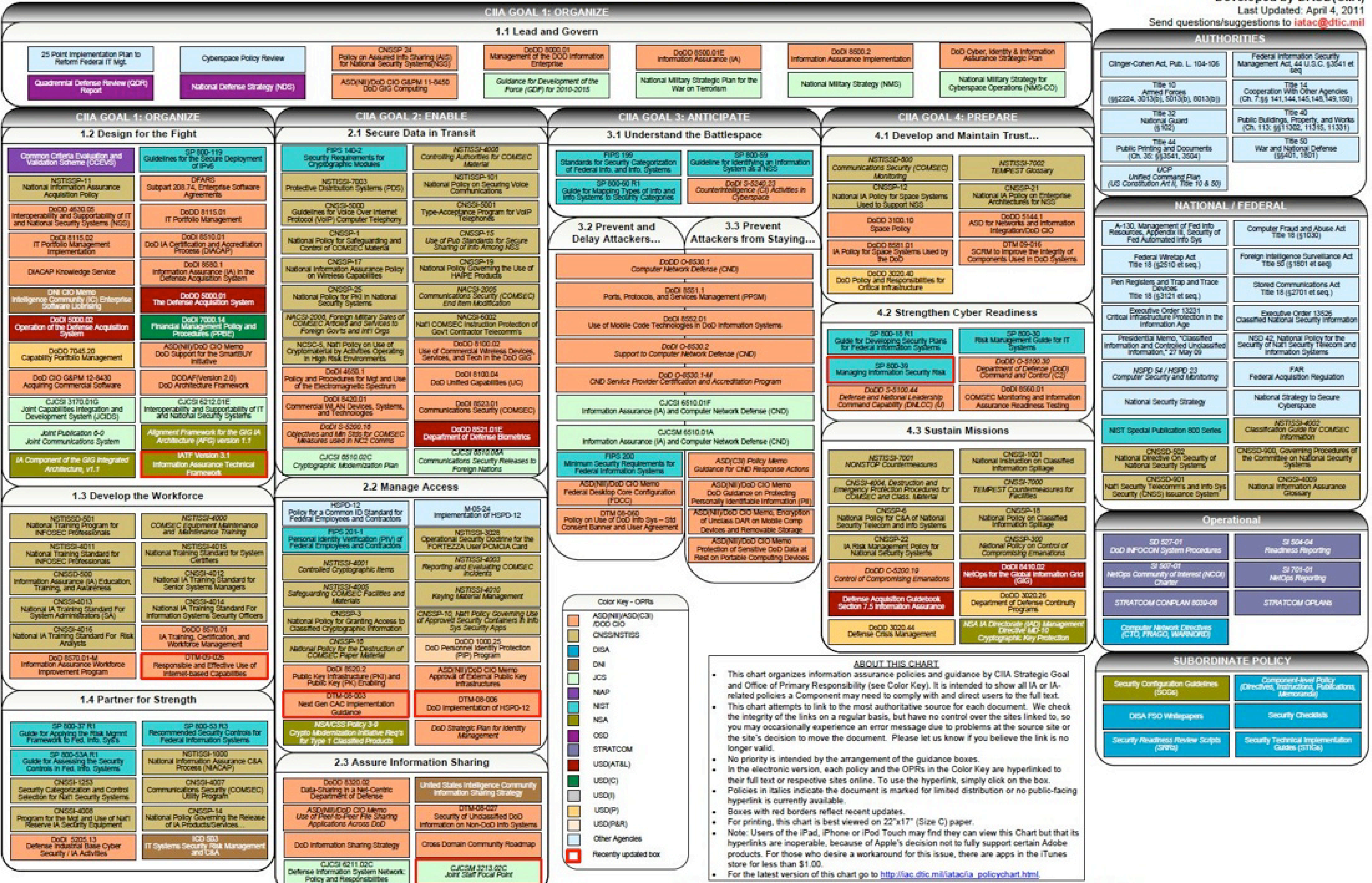


Top Down Structure

- “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.
- Quadrennial Defense Review (QDR) Report
- Cyberspace Policy Review
- National Defense Strategy (NDS)
- CNSSP 24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- ASD(NII)/DoD CIO G&PM 11-8450 DoD GIG Computing
- DoDD 8000.01 Management of the DOD Information Enterprise
- Guidance for Development of the Force (GDF) for 2010-2015
- DoDD 8500.01E Information Assurance (IA)
- National Military Strategic Plan for the War on Terrorism
- DoDI 8500.2 Information Assurance Implementation
- National Military Strategy (NMS)
- DoD Cyber, Identity & Information Assurance Strategic Plan
- 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 8580.1 Information Assurance (IA) in the Defense Acquisition System
- DNI 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 (PPBE)
- DoDD 7045.20 Capability Portfolio Management
- ASD(NII)/DoD CIO Memo DoD Support for the SmartBUY Initiative
- DoD CIO G&PM 12-8430 Acquiring Commercial Software
- DODAF(Version 2.0) DoD Architecture Framework
- CJCSI 3170.01G Joint Capabilities Integration and Development System (JCIDS)
- CJCSI 6212.01E Interoperability and Supportability of IT and National Security Systems
- *Joint Publication 6-0 Joint Communications System*
- *Alignment Framework for the GIG IA Architecture (AFG) 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

- NSTISSD-501 National Training Program for INFOSEC Professionals
- *NSTISSI-4000 COMSEC Equipment Maintenance and Maintenance Training*
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- CNSSI-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-09-026 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
- NSTISSI-1000 National Information Assurance C&A Process (NIACAP)
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- CNSSP-14 National Policy Governing the Release of IA Products/Services...
- DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities
- ICD 503 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
- *NSTISSI-4008 Controlling Authorities for COMSEC Material*
- NSTISSI-7003 Protective Distribution Systems (PDS)
- NSTISSP-101 National Policy on Securing Voice Communications
- CNSSI-5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- *CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS*
- CNSSP-17 National Information Assurance Policy on Wireless Capabilities
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- *NACSI-2008, Foreign Military Sales of COMSEC Articles and Services to Foreign Govts and Int'l Orgs*
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- NCSC-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 4650.1 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 S-5200.16 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 6510.06A Communications Security Releases 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
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- *NSTISSI-4001 Controlled Cryptographic Items*
- *NSTISSI-4003 Reporting and Evaluating COMSEC Incidents*
- *NSTISSI-4005 Safeguarding COMSEC Facilities and Materials*
- *NSTISSI-4010 Keying Material Management*
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- *CNSSP-10, Nat'l Policy Governing Use of Approved Security Containers in Info Sys Security Apps*
- *CNSSP-16 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 Focal 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 S-5240.23 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 O-8530.2 Support to Computer Network Defense (CND)*
- *DoD 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(NII)/DoD CIO Memo Federal Desktop Core Configuration (FDCC)
- DTM 08-060 Policy on Use of DoD Info Sys – Std Consent Banner and User Agreement
- *ASD(C3I) Policy Memo Guidance for CND Response Actions*
- ASD(NII)/DoD CIO Memo DoD Guidance on Protecting Personally Identifiable Information (PII)
- ASD(NII)/DoD CIO Memo, Encryption of Unclass DAR on Mobile Comp Devices and Removable Storage
- ASD(NII)/DoD CIO Memo Protection of Sensitive DoD Data at Rest on Portable Computing Devices

CIIA GOAL 4: PREPARE

4.1 Develop and Maintain Trust...

- *NSTISSD-600 Communications Security (COMSEC) Monitoring*
- *NSTISSI-7002 TEMPEST Glossary*
- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- DoDD 3100.10 Space Policy
- DoDD 5144.1 ASD for Networks and Information Integration/DoD CIO
- DoDD 8581.01 IA Policy for Space Systems Used by the DoD
- DTM 09-016 SCRM to Improve the Integrity of Components Used in DoD Systems
- DoDD 3020.40 DoD Policy and Responsibilities for Critical Infrastructure

4.2 Strengthen Cyber Readiness

- SP 800-18 R1 Guide for Developing Security Plans for Federal Information Systems
- SP 800-30 Risk Management Guide for IT Systems
- SP 800-39 Managing Information Security Risk
- *DoDD O-5100.30 Department of Defense (DoD) Command and Control (C2)*
- *DoDD S-5100.44 Defense and National Leadership Command Capability (DNLCC) (U)*
- DoDI 8560.01 COMSEC Monitoring and Information Assurance Readiness Testing

4.3 Sustain Missions

- *NSTISSI-7001 NONSTOP Countermeasures*
- CNSSI-1001 National Instruction on Classified Information Spillage
- *CNSSI-4004, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- CNSSP-6 National Policy for C&A of National Security Telecom and Info Systems
- CNSSP-18 National Policy on Classified Information Spillage
- CNSSP-22 IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- *DoDD C-5200.19 Control of Compromising Emanations*
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- Defense Acquisition Guidebook Section 7.5 Information Assurance
- DoDD 3020.26 Department of Defense Continuity Programs
- DoDD 3020.44 Defense Crisis Management
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*

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(b), 5013(b), 8013(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 III, 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 (§1801 et seq)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Executive Order 13231 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
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- FAR Federal Acquisition Regulation
- National Security Strategy
- National Strategy to Secure Cyberspace
- NIST Special Publication 800 Series
- *NSTISSI-4002 Classification Guide for COMSEC Information*
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 National Information Assurance Glossary

Operational

- *SD 527-01 DoD INFOCON System Procedures*
- *SI 504-04 Readiness Reporting*
- *SI 507-01 NetOps Community of Interest (NCOI) Charter*
- *SI 701-01 NetOps Reporting*
- *STRATCOM CONPLAN 8039-08*
- *STRATCOM OPLANS*
- *Computer Network Directives (CTO, FRAGO, WARNORD)*

SUBORDINATE POLICY

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

Color Key - OPRs

- ■ ASD(NII)/ASD(C3I)/DOD CIO
- ■ CNSS/NSTISS
- ■ DISA
- ■ DNI
- ■ JCS
- ■ NIAP
- ■ NIST
- ■ NSA
- ■ OSD
- ■ STRATCOM
- ■ USD(AT&L)
- ■ USD(C)
- ■ USD(I)
- ■ USD(P)
- ■ USD(P&R)
- ■ Other Agencies
- □ Recently updated box

ABOUT THIS CHART

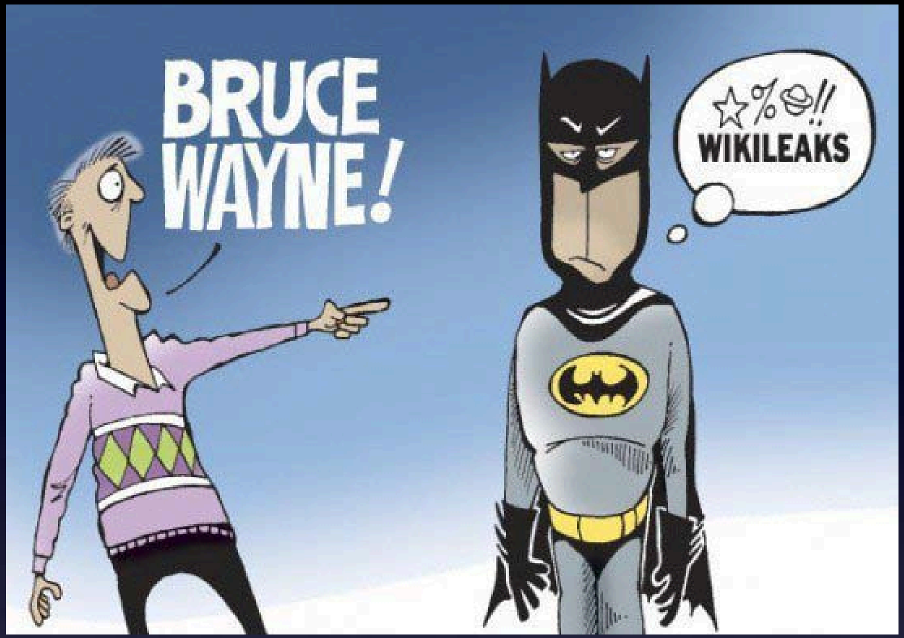
- This chart organizes information assurance policies and guidance by CIIA Strategic Goal and Office of Primary Responsibility (see Color Key). It is intended to show all IA or IA-related policies a Component may need to comply with and direct users to the full text.
- This chart attempts to link to 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.

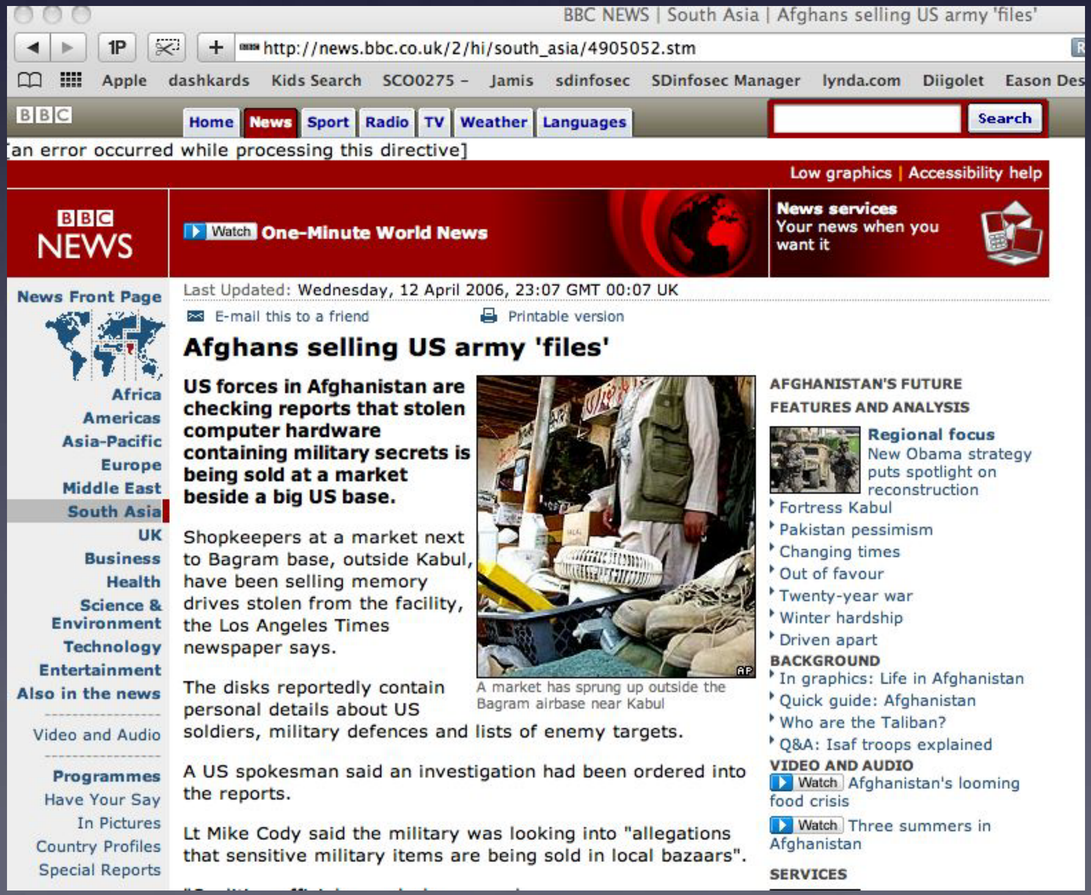
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

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 sdinfosec SDinfosec Manager lynda.com Diigolet Eason Des
BBC
Home News Sport Radio TV Weather Languages
Search
Low graphics | Accessibility help
BBC NEWS
Watch One-Minute World News
News services Your news when you want it
News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news
Video and Audio
Programmes
Have Your Say
In Pictures
Country Profiles
Special Reports
E-mail this to a friend
Printable version
AP

[an error occurred while processing this directive]

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

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.

A market has sprung up outside the Bagram airbase near Kabul

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

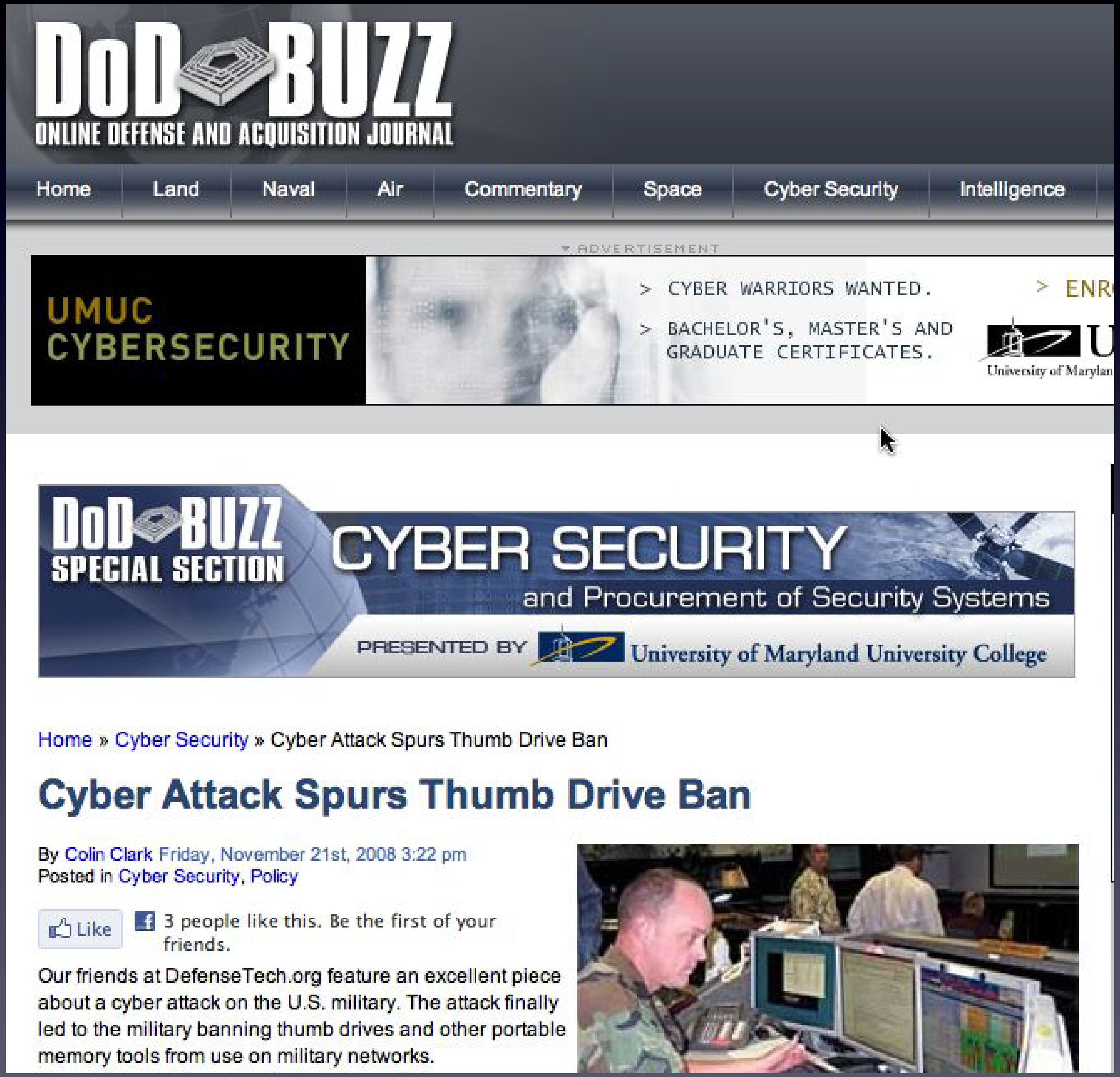
- In graphics: Life in Afghanistan
- Quick guide: Afghanistan
- Who are the Taliban?
- Q&A: Isaf troops explained

VIDEO AND AUDIO

Watch Afghanistan's looming food crisis

Watch Three summers in Afghanistan

SERVICES


DoD BUZZ
ONLINE DEFENSE AND ACQUISITION JOURNAL
Home
Land
Naval
Air
Commentary
Space
Cyber Security
Intelligence
DoD BUZZ SPECIAL SECTION
CYBER SECURITY
and Procurement of Security Systems
PRESENTED BY University of Maryland University College
Like

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

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

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