

# Build and Operate a Trusted GIG

## IIA GOAL 1: ORGANIZE

### 1.1 Lead and Govern

U.S. Int'l Strategy for Cyberspace	Cyberspace Policy Review	25 Point Implementation Plan to Reform Federal IT Mgt.	Quadrennial Defense Review (QDR) Report	National Defense Strategy (NDS)	CNSSP-24 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 Strategy for Operating in Cyberspace	DoD Cyber, Identity & Information Assurance Strategic Plan	DTM-01-001 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)

## Identity & Information Assurance-Related Policies and Issuances

Developed by the DoD CIO, IIA Deputate

Last Updated: January 5, 2012

Send questions/suggestions to [iatac@dtic.mil](mailto:iatac@dtic.mil)

## IIA GOAL 1: ORGANIZE

### 1.2 Design for the Fight

SP 800-119 Guidelines for the Secure Deployment of IPv6	Common Criteria Evaluation and Validation Scheme (CCEVS)
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 5000.01 The Defense Acquisition System
DoDD 7045.20 Capability Portfolio Management	DoDD 8115.01 IT Portfolio Management
DoDI 5000.02 Operation of the Defense Acquisition System	DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
DoDI 8115.02 IT Portfolio Management Implementation	DoDI 8510.01 DoD IA Certification and Accreditation Process (DIACAP)
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System	DIACAP Knowledge Service
DNI CIO Memo Intelligence Community (IC) Enterprise Software Licensing	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

CNSSD-500 Information Assurance (IA) Education, Training, and Awareness	NSTISSD-501 National Training Program for INFOSEC Professionals
NSTISSI-4000 COMSEC Equipment Maintenance and Maintenance Training	NSTISSI-4011 National Training Standard for INFOSEC Professionals
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	NSTISSI-4015 National Training Standard for System Certifiers
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

CNSSP-14 National Policy Governing the Release of IA Products/Services...	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	DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities
ICD 503 IT Systems Security Risk Management and C&A	

## IIA GOAL 2: ENABLE

### 2.1 Secure Data in Transit

FIPS 140-2 Security Requirements for Cryptographic Modules	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 HA/PE Products	CNSSP-25 National Policy for PKI in National Security Systems
NSTISSP-101 National Policy on Securing Voice Communications	NACSI-2005 Communications Security (COMSEC) End Item Modification
NSTISSI-4006 Controlling Authorities for COMSEC Material	CNSSI-5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony
CNSSI-5001 Type-Acceptance Program for VoIP Telephones	NACSI-6001, Foreign Military Sales of COMSEC Articles and Services to Foreign Gov'ts and Int'l Orgs
NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's	NSTISSI-7003 Protective Distribution Systems (PDS)
DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG	DoDD 8521.01E Department of Defense Biometrics
DoDI 4650.01 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	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	CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
CNSSP-16 National Policy for the Destruction of COMSEC Paper Material	NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
NSTISSI-4001 Controlled Cryptographic Items	NSTISSI-4003 Reporting and Evaluating COMSEC Incidents
NSTISSI-4010 Keying Material Management	CNSSI-4005 Safeguarding COMSEC Facilities and Materials
DoDD 1000.25 DoD Personnel Identity Protection (PIP) Program	DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
DoDI 8520.03 Identity Authentication for Information Systems	DTM-08-003 Next Gen CAC Implementation Guidance
DoD Strategic Plan for Identity Management	

### 2.3 Assure Information Sharing

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

## IIA 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	SP 800-92 Guide to Computer Security Log Management
NISTIR 7693 Specification for Asset Identification 1.1	DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

### 3.2 Prevent and Delay Attackers... and 3.3 Prevent Attackers from Staying...

FIPS 200 Minimum Security Requirements for Federal Information Systems	SP 800-37 R1 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
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
SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems	DoDD O-8530.1 Computer Network Defense (CND)
DoDI O-8530.2 Support to 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	DoD O-8530.1-M CND Service Provider Certification and Accreditation Program
DTM-08-060 Policy on Use of DoD Info Sys - Std Consent Banner and User Agreement	ASD(NII)/DoD CIO Memo Federal Desktop Core Configuration (FDCC)
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
CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)	CJCSM 6510.01A Information Assurance (IA) and Computer Network Defense (CND)

#### 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.
- 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](http://iac.dtic.mil/iatac/ia_policychart.html).

## IIA GOAL 4: PREPARE

### 4.1 Develop and Maintain Trust...

CNSSP-12 National IA Policy for Space Systems Used to Support NSS	CNSSP-21 National IA Policy on Enterprise Architectures for NSS
NSTISSD-600 Communications Security (COMSEC) Monitoring	NSTISSI-7002 TEMPEST Glossary
DoDD 3100.10 Space Policy	DoDD 3020.40 DoD Policy and Responsibilities for Critical Infrastructure
DoDD 5144.1 ASD for Networks and Information Integration/DoD CIO	DoDI 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	

### 4.2 Strengthen Cyber Readiness

SP 800-18 R1 Guide for Developing Security Plans for Federal Information Systems	SP 800-126 R2 SCAP Ver. 1.2
SP 800-30 Risk Management Guide for IT Systems	SP 800-39 Managing Information Security Risk
SP 800-137 Continuous Monitoring	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

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
CNSSI-1001 National Instruction on Classified Information Spillage	CNSSI-4004.1 Destruction and Emergency Protection Procedures for COMSEC and Class. Material
CNSSI-7000 TEMPEST Countermeasures for Facilities	NSTISSI-7001 NONSTOP Countermeasures
DoDD 3020.26 Department of Defense Continuity Programs	DoDD 3020.44 Defense Crisis Management
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	NSA IA Directorate (IAD) Management Directive MD-10 Cryptographic Key Protection

#### Color Key - OPRs

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

## AUTHORITIES

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)
Federal Information Security Management Act, 44 U.S.C. §3541 et seq	Title 50 War and National Defense (§§401, 1801)
Clinger-Cohen Act, Pub. L. 104-106	UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

## NATIONAL / FEDERAL

Computer Fraud and Abuse Act Title 18 (§1030)	Federal Wiretap Act Title 18 (§2510 et seq.)
Stored Communications Act Title 18 (§2701 et seq.)	Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)	Executive Order 13231 Critical Infrastructure Protection in the Information Age
Executive Order 13526 Classified National Security Information	Executive Order 13587 Structural Reforms To Improve Classified Nets
NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems	NSPD 54 / HSPD 23 Computer Security and Monitoring
Presidential Memo, "Classified Information and Controlled Unclassified Information," 27 May 09	A-130, Management of Fed Info Resources, Appendix III, Security of Fed Automated Info Sys
FAR Federal Acquisition Regulation	Ethics Regulations
National Security Strategy	National Strategy to Secure Cyberspace
NIST Special Publication 800 Series	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 Telecom's and Info Sys Security (CNSS) Issuance System
NSTISSI-4002 Classification Guide for COMSEC Information	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)