DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JUN 1 6 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

SUBJECT: Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance"

In a memorandum, "Global Information Grid," dated September 22, 1999, the Department of Defense (DoD) Chief Information Officer (CIO) issued guidance on the definition and scope of the Global Information Grid (GIG). In essence, the GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."

The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of GIG policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, enterprise computing.

U07251 /00

The attached Guidance and Policy for GIG Information Assurance (IA) provides direction and assigns responsibilities for secure, interoperable information capabilities that meet both warfighting and business needs. It provides the framework for achieving IA by ensuring the availability of systems, the integrity and confidentiality of information, and the authentication and non-repudiation of electronic transactions. The accompanying GIG IA Implementation Guidance provides details on the selection of appropriate security countermeasures required to secure the GIG architecture.

Some of the measures called for in the attached guidance and policy cannot be fully implemented immediately, however, the cyber threats and vulnerabilities to DoD information technology are such that implementation should begin immediately where possible. Subsequent guidance will establish final dates for the completion of specific measures. These dates will take into account the urgency and priority of the IA need and the projected availability of adequate IA solutions.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy and guidance is effective immediately, the DoD CIO, in coordination with the Director, Administration and Management, will incorporate it into the DoD Directive System within 180 days.

Please direct any questions to Mr. Donald L. Jones in the Office of the Director for Infrastructure and Information Assurance. He can be reached at (703) 614-6640 or e-mail: donald.l.jones@osd.pentagon.mil.

Rudy de Leon

Rudy de Leon

Attachments

Guidance and Policy for Department of Defense Global Information Grid Information Assurance

ASD (C3I)

References: (a) DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001- March 31, 2000 – Global Information Grid
(b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
(c) DoD 5200.28-M, "ADP Security Manual," January 1973 and Change 1, June 24, 1979
(d) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990.
(e) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999
(f) through (x), see Enclosure 1.

1. PURPOSE: This guidance and policy establishes Department of Defense (DoD) Global Information Grid (GIG) information assurance (IA) policy under (reference (a)), assigns responsibilities, and authorizes publication of implementation guidance to enable the secure exchange and use of information necessary to the execution of the DoD mission. This issuance specifically: establishes information system mission categories; defines levels of concern and corresponding levels of robustness and specifies requirements for their use; and, defines and directs implementation of a defense-in-depth strategy for applying integrated, layered protection of the DoD's information systems and networks. It supplements DoD Directive 5200.28, DoD Manual 5200.28-M, and DoD Directive C-5200.5 (references (b), (c), and (d)).

2. APPLICABILITY AND SCOPE:

2.1. This guidance and policy applies to:

2.1.1. The Office of the Secretary of Defense (OSD); the Military Departments; the Chairman of the Joint Chiefs of Staff; the Combatant Commands; the Inspector General of the Department of Defense (IG,DoD); the Defense Agencies and DoD field activities (hereafter referred to collectively as "the DoD Components").

2.1.2. Information technology and its operation by DoD Intelligence Agencies, Service intelligence elements and other intelligence activities engaged in direct support of Defense missions. Global Information Grid implementation must comply with policy and responsibilities established herein and, whenever applicable, separate and coordinated Director of Central Intelligence (DCI) directives and Intelligence Community (IC) policy.

2.1.3. All information technologies that are used to process, store, display or transmit DoD information, regardless of classification or sensitivity.

2.2. Additional measures may be required for the protection of foreign intelligence or counterintelligence information, Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI) (reference (f)), and Special Access Program (SAP) information (reference (g)) on DoD information systems and networks.

2.3. This policy does not apply to information systems to which reference (e) applies, i.e., Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI. Policies and procedures for the protection of IC information contained in information systems not covered by reference (e) shall be established through a process jointly determined between the DoD CIO and the IC CIO.

3. DEFINITIONS: Terms used in this issuance are defined in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009 (reference (h)) or at Enclosure 2.

4. POLICY: It is DoD policy that:

4.1. The DoD shall follow an enterprise-wide IA architectural overlay that is consistent with the overall Global Information Grid (GIG) Architecture, and implements a defense-in-depth strategy to establish and maintain an overall acceptable IA posture across the GIG. Protection mechanisms shall be applied such that information and information systems maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based on mission category, classification or sensitivity of information handled (i.e., processed, stored, displayed, or transmitted) by the system, and need-to-know, while maintaining required levels of interoperability. A companion issuance, Information Assurance Implementation Guidance, provides details on the selection and implementation of protection mechanisms.

4.2. All GIG information systems shall be assigned to a mission category (mission critical, mission support, or administrative) that reflects the type of information handled by the system relative to requirements for integrity (including authentication and non-repudiation) and availability services. Mission categories will be determined by the DoD functional domain owner or the responsible DoD Component Head in consultation with the information producer. The mission category of systems that handle information from multiple domains shall default to the highest category supported. System mission categories, functional domain, and information producer are defined in Enclosure 2, Definitions.

4.3. All GIG information systems shall employ protection mechanisms in accordance with the level of concern (i.e., high, medium, or basic) that satisfy corresponding criteria for high, medium, or basic levels of robustness. Paragraph 5 of the Information Assurance Implementation Guidance provides an in-depth discussion of levels of robustness and detailed guidance on their application to IA solutions within the following guidelines.

4.3.1. GIG information systems processing classified information as defined by DoD Regulation 5200.1-R (reference (i)) are assigned a high level of concern. Such systems shall employ only National Security Agency (NSA) certified high robustness IA

products when the information transits public networks or the system or network handling the information is accessible by individuals who are not cleared for the classified information on the system.

4.3.2. GIG information systems that meet the criteria of national security systems as delineated by Title 10, United States Code, Section 2315 (reference (j)) and process only unclassified information are assigned a medium level of concern and shall employ IA products that satisfy the requirements for at least medium robustness when the information transits public networks or the system or network handling the information is accessible by individuals who are not authorized to access the information on the system.

4.3.3. GIG information systems processing sensitive information as defined in section 20 of the National Institute of Standards and Technology Act (Title 15, United States Code, Section 278g-3 (reference (k)) are assigned a basic level of concern and shall employ IA products that satisfy the requirements for at least basic robustness when the information transits public networks or the system or network handling the information is accessible by individuals who are not authorized to access the information on the system.

4.3.4. GIG information systems that allow open, uncontrolled access to information through publicly accessible web servers or unregulated access to and from the Internet shall employ mechanisms to ensure availability and protect the information from malicious tampering or destruction. Such systems shall also be isolated from all other GIG systems. The isolation may be physical, or may be implemented by technical means such as an approved boundary protection product.

4.4. The DoD defense-in-depth strategy shall be implemented using technical solutions where possible in order to:

4.4.1. Ensure network and infrastructure services provide appropriate confidentiality (e.g., link encryption, one-time passwords, virtual private networks (VPN)) and defenses against denial of service attacks (e.g., diversity, routing table protection, and planned degraded operation).

4.4.2. Defend the perimeters of well-defined information enclaves (e.g., firewalls, intrusion detection, and a uniform policy on protocols allowed across perimeter boundaries).

4.4.3. Provide appropriate degrees of protection to all computing environments (e.g., internal hosts and applications).

4.4.4. Make appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, and directories).

4.5. All GIG information systems and networks shall be certified and accredited in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40 (reference (l)).

4.6. All inter-connections of GIG information systems, both internal and external, shall be managed to continuously minimize community risk and ensure that the protection of one system is not undermined by vulnerabilities of other interconnected systems. Further:

4.6.1. Interconnection of DoD systems at the same classification level shall be managed so that mutual risk is minimized.

4.6.2. Interconnections of DoD systems operating at different classification levels shall be accomplished consistent with the philosophy of the Secret and Below Interoperability (SABI) process (reference (m)) using criteria that have been approved by the DoD CIO and, where appropriate, formally coordinated with the IC CIO.

4.6.3. All connections to non-GIG information systems, including foreign nation and contractor systems, shall be accomplished in accordance with approved DoD criteria and be coordinated with the IC CIO, as appropriate.

4.7. Interconnections of IC systems and DoD systems shall be accomplished using a process jointly concurred in by the DoD CIO and the IC CIO.

4.8. Only COMSEC equipment acquired through NSA as the centralized COMSEC acquisition authority, or through NSA designated agents, shall be used to protect classified systems.

4. 9. All security related commercial-off-the-shelf (COTS) hardware, firmware, and software components (excluding cryptographic modules) required to protect GIG information systems, including those used to protect "Sensitive" information, shall be acquired in accordance with the guidance and schedule specified in the National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products (reference (n)), relevant portions of which are quoted at Enclosure 3. All government-off-the-shelf (GOTS) products of this nature shall be evaluated by NSA, or in accordance with NSA approved processes.

4.10. Public domain software products (i.e., freeware) shall not be used in GIG information systems unless an official requirement is established, the product is assessed for information assurance impacts, and approved for use by the responsible Designated Approving Authority (DAA).

4.11. Access to GIG information systems shall be granted to individuals based on need-to-know and in accordance with DoD Regulation 5200.2-R (reference (o)) for clearance, special access and ADP category designation requirements and qualifications.

4.12. Exchange of unclassified information between DoD and its vendors and contractors requiring IA services using public key techniques will be accomplished through External Certificate Authorities (ECAs). The ECAs will operate under a process which

delivers a level of assurance that meets business and legal requirements as determined by the DoD CIO in coordination with the DoD Comptroller and the DoD General Counsel.

4.13. GIG information systems shall be monitored in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security of DoD operations or information technology resources, including internal misuse.

4.14. All GIG information systems are subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD Directive 4640.6 (reference (p)), and other applicable laws and regulations.

4.15. Component General Counsel approved notice of privacy rights and security responsibilities shall be provided to all individuals attempting access to GIG information systems.

4.16. Use of public key certificates in GIG information systems shall be in accordance with the DoD public key infrastructure policy (reference (q)) and associated guidance.

4.17. All DoD personnel and support contractors shall be trained and appropriately certified to perform the tasks associated with their designated responsibilities for safeguarding and operating GIG information systems in accordance with joint USD (P&R) and ASD (C3I) guidance (reference (r)).

4.18. Mobile code technologies shall be categorized and their use restricted in order to reduce the threat to GIG information systems posed by malicious code.

4.19. Management of networks and management of IA operations (i.e., Computer Network Defense (CND)) shall be fully coordinated and co-located to the extent possible.

5. RESPONSIBILITIES:

5.1. The DoD Chief Information Officer (CIO) shall:

5.1.1. Ensure that this policy is implemented in the context of the GIG Architecture.

5.1.2. Develop and promulgate additional DoD IA related policy and guidance on specific topics in support of, and consistent with, this issuance (e.g., defense-in-depth, mobile code, web sites, monitoring and testing).

5.1.3. Ensure that all GIG information systems are assigned to a mission category.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection (reference (s)) sector liaisons.

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the DoD.

5.1.6. Manage the Defense-wide IA Program (DIAP), that shall:

5.1.6.1. Provide for the planning, coordination, integration, and oversight of all DoD IA activities.

5.1.6.2. Establish and monitor IA readiness as an integral part of the DoD mission readiness criteria.

5.1.6.3. Maintain liaison with the office of the IC CIO to ensure continuous coordination of DoD and IC IA activities and programs.

5.1.7. Appoint Designated Approving Authorities (DAAs) for all new Enterprise-wide information systems and confirm DAAs for existing Enterprise-wide systems (e.g., Global Command and Control System, Defense Message System, Defense Travel System).

5.2. The Heads of DoD Components shall:

5.2.1. Develop and implement an IA program consistent with the GIG IA architectural overlay and the DoD defense-in-depth strategy focusing on protection of Component-specific information and systems (i.e., sustaining base, tactical, C4I interfaces to weapon systems).

5.2.2. Secure information systems and networks in accordance with the assigned level of concern by acquiring and employing IA solutions in accordance with reference (n) and the robustness policies described in the Information Assurance Implementation Guidance.

5.2.3. Appoint Designated Approving Authorities (DAAs) and ensure they accredit each information system under their jurisdiction and implement IA solutions indicated by the results of the risk assessment process outlined in the DITSCAP, (reference (l)) to insure proper IA risk management and sustainment.

5.2.4. Comply with established connection approval processes for all information systems connections and develop Memorandums of Agreement (MOA) with other Component Heads, as appropriate, for interconnection of information systems managed by multiple DAAs.

5.2.5. Assign mission categories to Component-specific systems.

5.2.6. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all system technologies and supporting infrastructures, including sustaining base, tactical, and C4I interfaces to weapon systems.

5.2.7. Ensure that IA awareness, training, education, and professionalization are provided to all military and civilian personnel, including contractors, commensurate with their respective responsibilities for using, operating, administering, and maintaining GIG information systems, in accordance with reference (r).

5.2.8. Share techniques, technologies, R&D, and lessons learned relating to IA with other DoD Components.

5.2.9. Provide for an IA monitoring and testing capability in accordance with DoD Directive 4640.6 (reference (p)) and applicable laws and regulations.

5.2.10. Provide for vulnerability mitigation and an incident response and reporting capability in order to:

5.2.10.1. Take appropriate actions in response to IA vulnerability alert notifications issued through the Information Assurance Vulnerability Alert (IAVA) Process (reference (t)).

5.2.10.2. Report all systems security incidents in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01B (reference (u)).

5.2.10.3. Take action in response to Information Operation Conditions (INFOCONs) as directed under reference (v).

5.2.10.4. Take actions necessary to limit damage and restore effective service following a computer network attack (CNA) or computer network exploitation (CNE).

5.2.10.5. Collect and retain audit data to support forensics relating to misuse, penetration reconstruction, or other investigations.

5.2.11. Comply with DoD COMSEC instructions and regulations.

5.2.12. Ensure that requirements to protect classified and sensitive unclassified information are placed in contracts and monitor contractors for compliance.

5.2.13 Ensure that all COTS and GOTS components required for security functions (excluding cryptographic modules) are acquired in accordance with the guidance and schedule specified in the National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Products, (reference (n)).

5.2.14. Consult the IA Technical Framework (IATF) (http://www.iatf.net) and published Common Criteria (CC) Protection Profiles for guidance regarding common classes of network and system attacks, interoperability and compatibility with the defense-in-depth strategy, and IA solutions that should be considered to counter attacks.

5.2.15. Ensure that access to GIG information systems and to specified types of information (e.g., intelligence, proprietary) under their jurisdiction is granted only on a need to know basis and that all personnel having access are appropriately cleared or qualified under the provisions of DoD Regulation 5200.2-R (reference (o)).

5.2.16. Ensure that PKI implementations follow policy as stated in the DoD PKI policy (reference (q)) and associated guidance.

5.2.17 Ensure that appropriate warnings are provided to all individuals accessing Component owned or controlled information systems.

5.2.18. Ensure coordination of management of IA operations (i.e., CND) with network management and co-locate the two functions when possible.

5.3. The OSD Principal Staff Assistants, in addition to the responsibilities specified in paragraph 5.2, shall ensure that IA requirements for information systems and functional applications developed under their cognizance are fully coordinated at the DoD Component level.

5.4. The Chairman, Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.2., shall:

5.4.1. Ensure that Combatant Commanders incorporate appropriate IA elements in the generation of requirements for systems support to Joint and Combined operations.

5.4.2. Validate requirements for non-DoD (e.g., Department of State) and foreign nation access to DoD-wide elements of the GIG prior to their submission to the appropriate connection approval process.

5.5. The Commander, JTF-CND, under USCINCSPACE, shall:

5.5.1. Coordinate and direct DoD-wide computer network defense operations to include:

5.5.1.1. Actions necessary to synchronize the defense of DoD computer systems and networks (e.g., network patches, firewall rules).

5.5.1.2. Actions necessary to stop a computer network attack (CNA) or computer network exploitation (CNE), limit damage from such activities, and coordinate the restoration of effective computer network service following a CNA or CNE.

5.5.2. Declare changes in INFOCON and issue INFOCONs in accordance with Chairman of the Joint Chiefs of Staff Memorandum CM-510-99, "Information Operations Condition (INFOCON)" (reference (v)).

5.6. The Director, National Security Agency (NSA), in addition to responsibilities specified in paragraph 5.2., shall:

5.6.1. Implement an IA intelligence capability responsive to requirements for the DoD, less DIA responsibilities.

5.6.2. Assess the risk to IA technologies, based on the threat to, and vulnerability of, such technologies.

5.6.3. Serve as the DoD focal point for INFOSEC R&D in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.6.4. Lead the development of the IA technical framework in support of the defense-in-depth strategy and provide engineering support and other technical assistance for its implementation within DoD.

5.6.5. Establish and manage a program for the evaluation and validation testing of commercially developed IA products in categories directed by the DoD CIO.

5.6.6. Certify cryptographic modules that are used to protect classified information and approve cryptographic modules that are used to protect unclassified information processed by national security systems as delineated by Title 10, United States Code, Section 2315 (reference (j)).

5.6.7. Serve as the DoD focal point for the National Information Assurance Partnership (NIAP). Through the NIAP, establish criteria and processes for evaluating and validating all security related commercial-off-the-shelf (COTS) firmware, and software components (excluding cryptographic modules) required to protect GIG information systems.

5.6.8. Coordinate activities of the National Security Incident Response Center (NSIRC) (reference (w)) with other DoD Components to integrate NSIRC efforts into protection of the enterprise.

5.6.9. Act as the centralized COMSEC acquisition authority.

5.7. The Director, Defense Intelligence Agency (DIA), in addition to the responsibilities specified in paragraph 5.2., shall:

5.7.1. Provide finished intelligence on IA, including threat assessments, to DoD Components.

5.7.2. Develop, implement, and oversee an IA program for layered protection of the DoD Intelligence Information System (DoDIIS).

5.7.3 Manage the connection approval process for Joint Worldwide Intelligence Communications System (JWICS) elements of the DISN in accordance with the process determined under paragraph 4.7., above.

5.8. The Director, Defense Information Systems Agency (DISA), in addition to the responsibilities specified in paragraph 5.2., shall:

5.8.1. Lead the development and implementation of a single IA strategy for defense-in-depth of the DoD-wide elements of the GIG, based on the IATF.

5.8.2. Establish connection requirements and manage connection approval processes for the long haul elements of the DISN (e.g., the Secret Internet Protocol Router Network (SIPRNET), the Unclassified But Sensitive Internet Protocol Network (NIPRNET), and the DISN Video Services Global (DVSG)).

5.8.3. Operate and maintain, in coordination with the other DoD Components, a DoD-wide information system monitoring and incident response center.

5.8.4. Coordinate with and support the JTF-CND, through USSPACECOM.

5.8.5. In coordination with the Joint Staff, NSA, and DIA as required, maintain security accreditation of the DoD-wide elements of the information infrastructure.

5.8.6. Coordinate the DoD Information Assurance Vulnerability Alert (IAVA) Process (reference (t)).

5.8.7. Maintain the DITSCAP (reference (l)) for security certification and accreditation of DoD component and contractor information technology systems.

5.8.8. In coordination with other DoD Components as required, develop and provide baseline DoD-level IA training and awareness products.

5.8.9. Perform the connection approval process for contractors requiring access to the Defense Information Systems Network (DISN).

5.9. The Director, Defense Security Service (DSS), in addition to the responsibilities specified in paragraph 5.2., shall:

5.9.1. Monitor information system security practices of DoD contractors processing classified information in accordance with DoD Directive 5220.22M (reference (x)).

5.9.2. Inspect COMSEC accounts as a part of regular industrial security inspections at DoD contractor facilities.

5.10. Each Designated Approving Authority (DAA) shall:

5.10.1. Establish and maintain the security of all systems under their jurisdiction.

5.10.2. Review and approve security safeguards and issue accreditation statements for each system under their jurisdiction, based on the acceptability of the safeguards and compliance with the DITSCAP (reference (l)).

5.10.3. Ensure that all required safeguards, as specified in accreditation documentation, are implemented and maintained.

5.10.4. Identify security deficiencies and initiate appropriate action to achieve an acceptable security level as required.

5.10.5. Ensure that Information Systems Security Managers (ISSMs), Information Systems Security Officers (ISSOs), and Systems Administrators (SAs) are designated for all systems under their jurisdiction, and that they receive the level of training necessary and appropriate certification to perform the tasks associated with their assigned responsibilities.

5.10.6. Verify that data ownership is established for each system under their jurisdiction and that the system has been assigned to a mission category.

5.10.7. Ensure that systems provide mechanisms for controlling access to specific information (e.g., intelligence, proprietary) based on mission and need-to-know determinations made by information producers.

5.10.8. Ensure that a process for reporting security incidents and lessons learned is established.

5.10.9. Be an employee of the U.S. Government.

5.11 Each Information Systems Security Manager (ISSM) shall:

5.11.1. Serve as the focal point for policy and guidance on IA matters within their activity.

5.11.2. Provide policy and program guidance to subordinate activities.

5.12. Each Information Systems Security Officer (ISSO) shall:

5.12.1. Ensure that systems for which they have cognizance are operated, used, maintained, and disposed of in accordance with the system accreditation package security policies and practices.

5.12.2. Within ISSO lines of authority, enforce IA policies and safeguards on all personnel having access to the system for which the ISSO has cognizance.

5.12.3. Ensure that users have the required security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with required security practices prior to being granted access to the system.

5.12.4. Ensure that audit trails are reviewed periodically.

5.12.5. Report all security incidents.

5.12.6. Report on the IA posture of the information system as required by the DAA.

5.13. Each System Administrator (SA) shall:

5.13.1. Work closely with the ISSO to ensure the system is used properly.

5.13.2. Assist the ISSO in maintaining system configuration controls and need-to-know information protection mechanisms.

5.13.3. Advise the ISSO of security anomalies or integrity deficiencies.

5.13.4. Administer, when applicable, user identification or authentication mechanisms of the system.

5.3.5. Perform system backups, software upgrades and system recovery, including the secure storage and distribution of backups and upgrades.

5.14. Each System User shall:

5.14.1. Observe regulations and guidance governing the secure operation (e.g., protection of passwords) and authorized use of an information system.

5.14.2. Immediately report all security incidents, potential threats and suspected vulnerabilities to the appropriate ISSO or ISSM.

6. EFFECTIVE DATE: This policy is effective immediately. In the event of conflicts between this policy and other IA related policy and guidance, this issuance takes precedence.

Enclosures – 3
1. References
2. Definitions
3. Policy Excerpt

(Encl. 1)

–E1 ENCLOSURE 1
REFERENCES

(f) SM-313-83, "Safeguarding the Single Integrated Operational Plan (U)," May 10, 1983

(g) DoD Directive O-5205.7 "Special Access Program (SAP) Policy," January 13,1997

(h) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009 rev 1, "National Information Systems Security Glossary," January 1999

(i) DoD Regulation 5200.1-R, "DoD Information Security Program," January. 1997

(j) Title 10, United States Code, Section 2315

(k) Title 15, United States Code, Section 278g-3

(l) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process," December 30, 1997.

(m) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, 'Secret and Below Interoperability (SABI)," March 20, 1997

(n) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products," January 2000

(o) DoD Regulation 5200.2-R, "Personnel Security Program," May 6, 1992

(p) DoD Directive 4640.6, "Communications Security (COMSEC) Monitoring and Recording," June 26, 1981

(q) Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," May 6, 1999

(r) Under Secretary of Defense (Personnel and Readiness) and Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Joint Memorandum, "Information Assurance (IA) Training and Certification," June 29, 1998

(s) Presidential Decision Directive/NSC –63, Subject: "Critical Infrastructure Protection," May 22, 1998

(t) Deputy Secretary of Defense (SECDEF) Memorandum, Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA) , December 30, 1999

(u) Chairman of the Joint Chiefs of Staff Instruction 6510.01B, "Defensive Information Operations Implementation", 22 August 1997, w/CH 1 26 August 1998

(v) Chairman of the Joint Chiefs of Staff Memorandum CM-510-99, "Information Operations Condition (INFOCON)", 10 March 1999

(w) National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 503, "Incident Response and Vulnerability Reporting for National Security Systems," August 30, 1993

(x) DoD Directive 5220.22M, "National Industrial Security Program Operating Manual," January 1995 and supplement, February 1995

(y) DCID 1/7, "Security Controls on the Dissemination of Intelligence Information," June 30, 1998

–E2. ENCLOSURE 2
DEFINITIONS

E2.1. Common Operating Environment. The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), runtime environment definitions, reference implementations, and methodology, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product. (DII COE I&RTS)

E2.2. Community Risk. A combination of: 1) the likelihood that a threat will occur within an interacting population; 2) the likelihood that a threat occurrence will result in an adverse impact to some or all members of that populace; and 3) the severity of the resulting impact. (SABI Terms of Reference (TOR))

E2.3. Connection Approval. Authorization to link or join a system with an existing network. (SABI TOR)

E2.4. Criticality. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing. (SABI Handbook)

E2.5. Defense-In- Depth. The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured.

E2.6. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (DoDI 5200.40)

E2.7. Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer.

E.2.8. Encryption. A procedure to convert plain text into cipher text. Within DoD, there are three reasons to encrypt:

a. Confidentiality. To ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes.

b. Data Separation. To ensure that information of different classifications sharing the same transport (transmission) media are not co-mingled.

c. Privacy. To ensure that information at the same classification level is kept separate based on need-to-know.

E2.9. External Certificate Authority. An agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities. Operating requirements for ECAs must be approved by the DoD CIO, in coordination with the DoD Comptroller and the OSD General Counsel. (DoD PKI Policy)

E2.10. Freeware. Also known as free software. Software that is free from licensing fees and has no restrictions on use; it can be freely copied, redistributed, or modified.

E2.11. Functional Domain. An identifiable DoD functional mission area. For purposes of this policy, the functional domains are: command and control, space, information operations, weapon systems. communications and broadcast, navigation, modeling and simulation, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and intelligence, surveillance, and reconnaissance (ISR) .

E2.12. Incident Detection and Response Capabilities. The establishment of mechanisms and procedures to monitor information systems and networks; detect, report and document attempted or realized penetrations of those systems and networks; and institute appropriate countermeasures or corrective actions.

E2.13. Information Assurance. Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1)

E2.14. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying CINCs, Services and agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. (JTF-CND CONOP)

E2.15. Information Operations Condition (INFOCON). The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system

presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack); BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions. (CJCS MEMO CM-510-00, 10 March 1999)

E2.16. Information Producer. A person, group, or organization that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions.

E2.17. Information System. The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information. (NSTISSI No. 4009)

E2.18. Intelligence Community Information: Sensitive Compartmented Information and any other intelligence information that is classified pursuant to section 1.5(c) of Executive Order 12958 that also bears special intelligence information control markings as required by DCID 1/7, "Security Controls on the Dissemination of Intelligence Information".

E2.19. Layered Defense. A combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers.

E2.20 Level of Concern. A rating assigned to an information system that indicates the extent to which protective measures, techniques, and procedures must be applied. The DoD has three levels of concern.

a. High: Information systems that require the most stringent protection measures and rigorous countermeasures.

b. Medium: Information systems that require layering of additional safeguards above the DoD minimum standard (Basic).

c. Basic: Information systems that require implementation of the DoD minimum standard.

E2.21. Level of Robustness. The characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly to support the level of concern assigned to a particular information system. DoD has three levels of robustness:

a. High: Security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures.

b. Medium: Security services and mechanisms that provide for layering of additional safeguards above the DoD minimum (Basic).

c. Basic: Security services and mechanisms that equate to good commercial practices.

E2.22. Mission Category. Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

a. Mission Critical. Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).[1]

b. Mission Support. Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

c. Administrative. Systems handling information which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

E2.23. Mobile Code: Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local systems without explicit installation or execution by the recipient. Malicious mobile code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources.

E2.24 National Information Assurance Partnership (NIAP). A collaboration between the National Institute of Standards and Technology (NIST) and NSA to meet the security testing needs of both information technology producers and users. The program is intended to foster the availability of objective measures and test methods for evaluating the quality of IT

[1] This definition of Mission Critical is operationally focussed and differs from that in the Clinger-Cohen Act of 1996 as well as the one used for reporting to congress under Section 8121 of the FY 2000 Defense Appropriations Act, both of which pertain to information technology procurement, not information or mission assurance support to deployed forces.

security products and provide a sound and reliable basis for the evaluation, comparison and selection of security products.

E2.25 National Security System. Any telecommunications or information system operated by the Department of Defense, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions, but not including a system, and equipment and services of a system, that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 10 U.S.C, Section 2315)

E2.26 Network Centric. A holistic view of interconnected information systems and resources that encourages a broader approach to security management than a component-based approach. (SABI TOR)

E2.27. Operating Environment. The total environment in which an information system operates. It includes the physical facility and controls, procedural and administrative controls, personnel controls (e.g., clearance level of the least cleared user).

E2.28. Public Key Infrastructure (PKI). An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

E2.29. Sensitive Information. "Sensitive" information is any information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DoD payroll, finance, logistics, and personnel management systems.
(NOTE: Certain information the disclosure of which would constitute an unwarranted invasion of personal privacy is exempt from mandatory disclosure under the Freedom of Information Act of 1974.)

E2.30. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (DCID 1/19)

E2.31. Secret and Below Interoperability (SABI) Initiative. An ASD (C3I) directed, JCS sponsored, NSA/DISA executed initiative to enhance Secret and Below Interoperability, measure community risk, and protect the GIG information systems infrastructure. (SABI Handbook)

(Encl. 3)

-E3 ENCLOSURE 3

Excerpt from the National Policy Governing the Acquisition of Information Assurance(IA) and IA-Enabled IT Products

SECTION I - POLICY

1. Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition appropriate implementation of evaluated or validated Government Off-the Shelf {GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the availability the systems, ensure the integrity and *confidentiality* of information, and the *authentication and non-repudiation* of parties in electronic transactions.

2. Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

a. The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

b. The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

c. The NIST Federal Information Processing Standard (FIPS) validation program.

The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

3. By 1 July 2002, the acquisition of all COTS IA and IA-enabled products to be used on the systems specified in paragraph 2., above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in subparagraphs 2.a. through 2.c.

4. The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

5. Normally, a complementary combination of lA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this. NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

6. Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 {PDD-63), Critical Infrastructures Protection.

SECTION II - RESPONSIBILITIES

7. Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

SECTION III - EXEMPTIONS AND WAIVERS

8. COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

9. Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the DIRNSA, ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary, to support U.S. Government operations which are t/me-sensitive, or where U.S. lives may be at risk.

Global Information Grid
Information Assurance Implementation Guidance

1. Purpose and Overview

This issuance provides guidance on implementing Global Information Grid (GIG) Policy 6-8510, Department of Defense Information Assurance. It addresses the selection of appropriate security countermeasures required to secure the GIG architecture. It describes the DoD defense-in-depth strategy, in which layers of defense are used to achieve the security objectives. It also points to the Information Assurance Technical Framework (IATF), which provides technical solutions and detailed implementation guidance for specific situations.

1.1. The guidance is divided into the following sections.

- Section 1 gives the purpose of the document, describes the sections, provides an overview of information assurance, and shows how IA relates to the overall GIG initiative.
- Section 2 describes the operational environment and defines and explains the purpose of mission categories.
- Section 3 addresses defense-in-depth, discusses target environments for the three major IT focus areas (i.e., networks, enclaves and boundaries, and the computing environment), and the security management infrastructure and provides tables that describe high level objectives for securing each focus area.
- Section 4 discusses the threat and attack environment and provides a table of common threats and categories of attacks that may target various components of the IT environment (i.e., networks, enclaves, hosts, applications).
- Section 5 discusses levels of robustness for individual security services and mechanisms and how they relate to overall IA solutions.
- Section 6 addresses non-technical countermeasures including: personnel, physical, and procedural security; security training, education and awareness; marking and labeling; incident reporting and response; assessments; and, risk management.

1.2. Information Assurance (IA) services provide security by ensuring the availability of the information system, the integrity and confidentiality of information and the accountability and non-repudiation of parties in electronic transactions. To the degree required, these IA services must be employed for all information and systems in the DoD (i.e., both classified and unclassified, and whether deemed mission critical, mission support or administrative). Further, the majority of DoD information systems are interconnected so that a security risk assumed by one entity is a risk shared by all those who are a part of the interconnected systems. Security is needed not only for intra-CINC, Service and Agency transactions, but also for transactions among the DoD components, and with other U.S. government departments, allies and trading partners. For these reasons, a comprehensive, common IA strategy becomes very important and all DoD components must cooperate in its development and implementation.

1.3 It is important to keep in mind that there are no "cookbook" solutions to appropriate IA. Any specific implementation is dependent upon an in-depth system security analysis and evaluation which must take into consideration all of the factors (e.g., system mission category, level of concern, confidentiality requirements, threat, and operating environment) in order to tailor an appropriate defense-in-depth solution for the implementation. Additional detail on security technologies that can satisfy defense-in-depth requirements may be found in the Information Assurance Technical Framework (http://www.iatf.net).

1.4. The need for securing DoD information and systems against the full spectrum of cyber threats dictates the use of multiple IA solutions that address people, technology and operations. The fundamental strategy principle is that layers of IA solutions are needed to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, any single system cannot be adequately secured unless all interconnected systems are adequately secured. Thus, an IA solution for any system must be considered within the context of the shared risk environment. The defense-in-depth strategy is also predicated on a sound IA technical framework, reflecting technical, performance, and best practice standards developed in conjunction with the IT industry. Thus, to the greatest extent possible, the recommendations of the IATF will leverage emerging commercial IA technology with available government IA technology. This guidance is structured in accordance with the defense-in-depth technical layers: the network and infrastructure, the enclave boundary, the computing environment, and the overarching security management infrastructure. Figure 1-2 below depicts defense-in-depth from technical, operational, and people related perspectives. The primary focus of this guidance is the technical implementation, however, operational and personnel aspects are discussed in Section 6.

Figure 1-2 Defense-in-Depth

1.5. The document tree in Figure 1-3 below describes the overall GIG Information Assurance effort and shows the policy and guidance provided at different levels within the DoD. As the user goes down through the layers of the tree, the technical implementations more fully describe and support the capability to design security into systems during the development and acquisition processes.

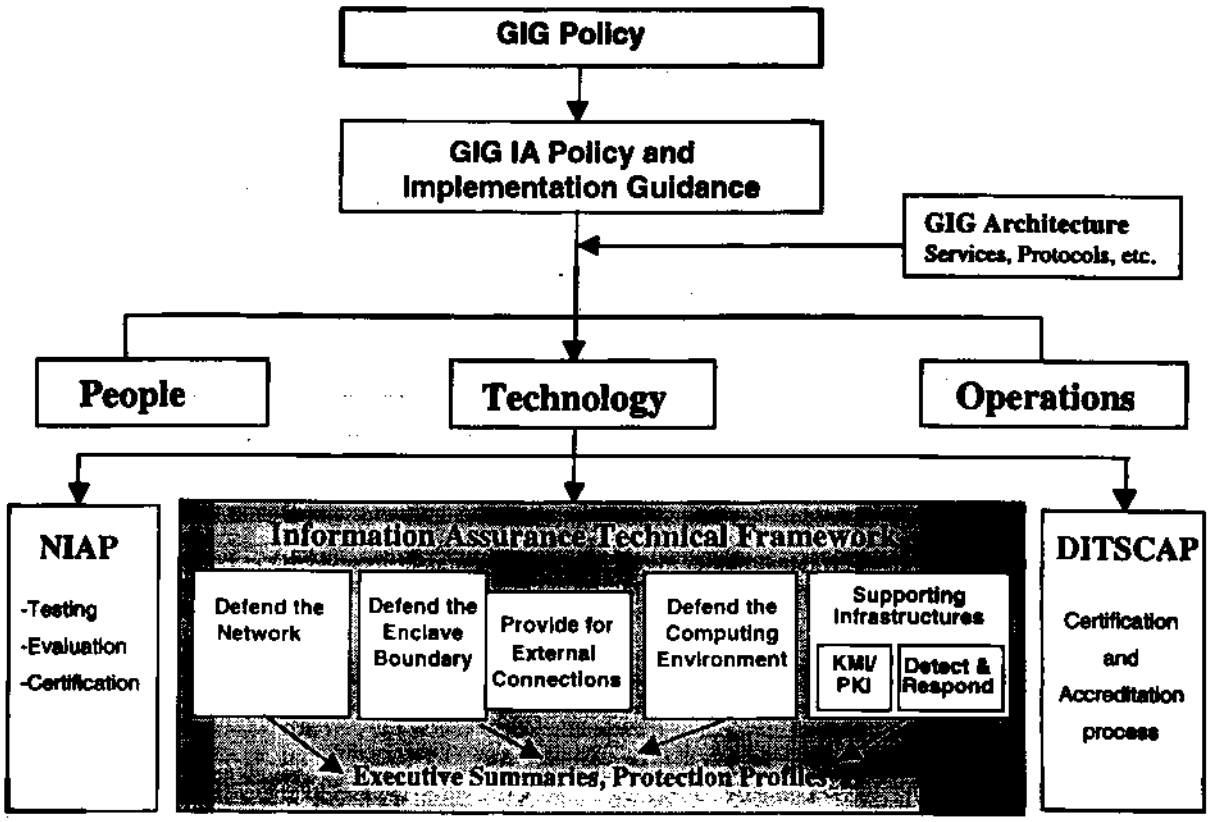

Figure 1-3 GIG IA Document Tree

2. Operational Environment and Mission Categories

2.1. Operational Environment: The DoD operates many systems that pass information on commercial network infrastructures between local enclaves. Enclaves typically contain multiple local area networks (LANs) with computing assets such as workstations (users), printers, servers, and switching/routing components, which transmit, process, and store information and support necessary services such as intrusion detection and virus detection. The wide area network (WAN) contains components such as routers and switches, which direct the flow of information through the infrastructure. The infrastructure contains the transmission components (satellites, microwave, other RF spectrum, fiber, etc.), most of it commercially leased, to move information across the network. DoD employs the Internet and public switched telephone network backbones, as well as the radio frequency spectrum for voice and data transmission. Figure 2-1 represents today's operating environment from a high level networking perspective. Detailed defense in depth layers are defined in section 3.

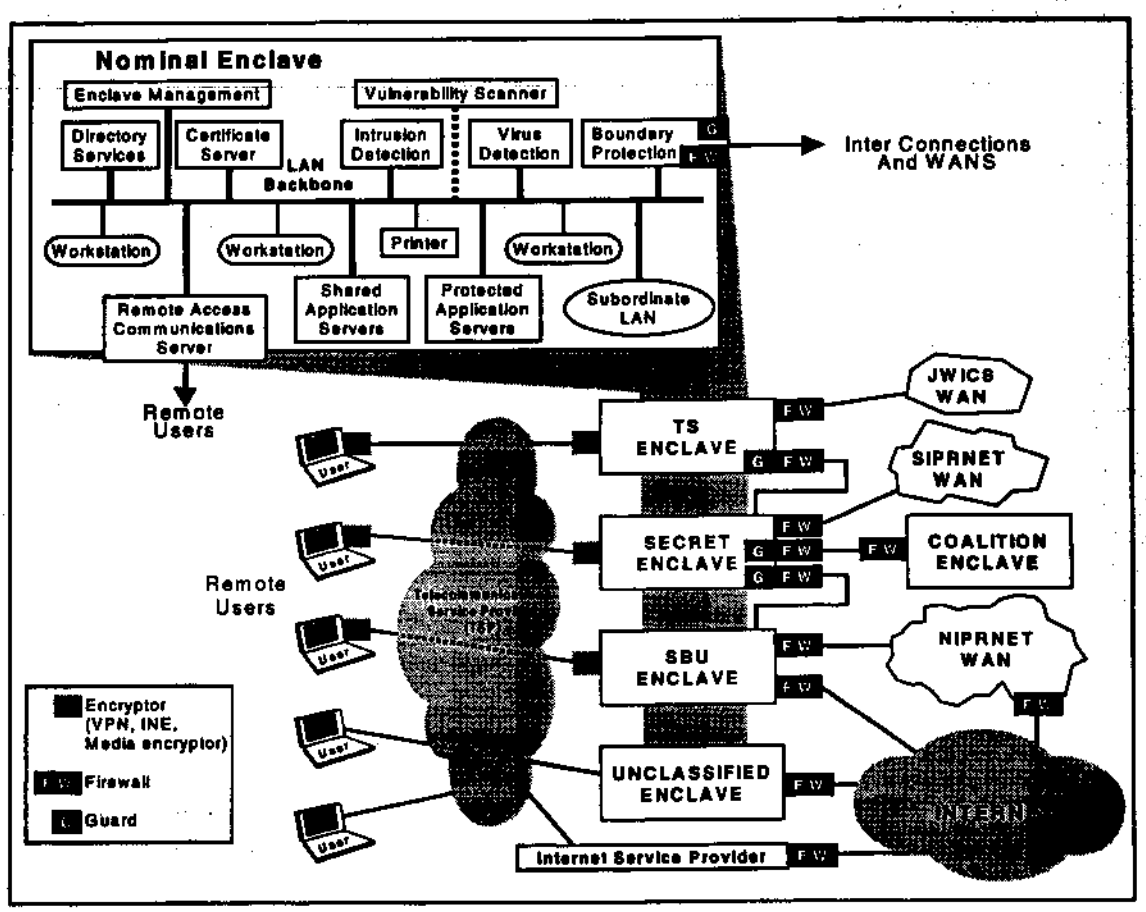

Figure 2-1 Operational Environment

2.2. Information transmitted, processed or stored in the operational environment described above is currently hierarchically "classified" as Top Secret/ SCI, Top Secret, Secret, Confidential, Sensitive, or Unclassified. In addition, information can be further tagged with a number of handling caveats.

2.3. Mission Categories: While the long standing hierarchical classification scheme is useful for identifying confidentiality needs, it is not very useful in identifying needs for other IA services such as system availability, integrity, and authentication and nonrepudiation. Thus, in addition to classification, information and systems within this environment need to be categorized as Mission Critical, Mission Support or Administrative. Mission categories provide the basis for determining the robustness requirements for availability and integrity services, and are significant from both cost and operational perspectives. They provide a means for prioritizing IT support and allocating resources based on needs for system availability and integrity services. These categories are defined as follows.

2.3.1. Mission Critical: These systems handle information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified, sensitive, or unclassified information).

2.3.2. Mission Support: These systems handle information important to the support of deployed and contingency forces. Information on these systems must be accurate, but can sustain minimal delays without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

2.3.3. Administrative: These systems handle information which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified but is usually sensitive or unclassified). It is recognized that this information may be recreated if the need arises.

3. Defense in Depth

The concept of defense-in-depth was presented in the overview section of this document. This section describes the four focus areas of defense-in-depth, discusses target environments and proposes objectives for assurance of each focus area.

3.1 Defend the Network: Networks and their supporting infrastructures include large transport networks and other transmission and switching capabilities. They include operational area networks (OANs), metropolitan area networks (MANs), campus area networks (CANs), and local area networks (LANs), extending coverage from broad communities to local bases. Figure 3-1 depicts a high level view of defense of the network with suggested placement for information assurance components and mechanisms. Table 3-1 lists high level objectives for defending the network and infrastructure and should be used to define solutions sets in the architecture framework. The target environment for network defense includes data, voice, wireless (e.g. cellular, paging), and tactical networks that support both the operational and strategic DoD missions. These networks can be DoD owned and operated (both service and transport) or leased services (transport layer).

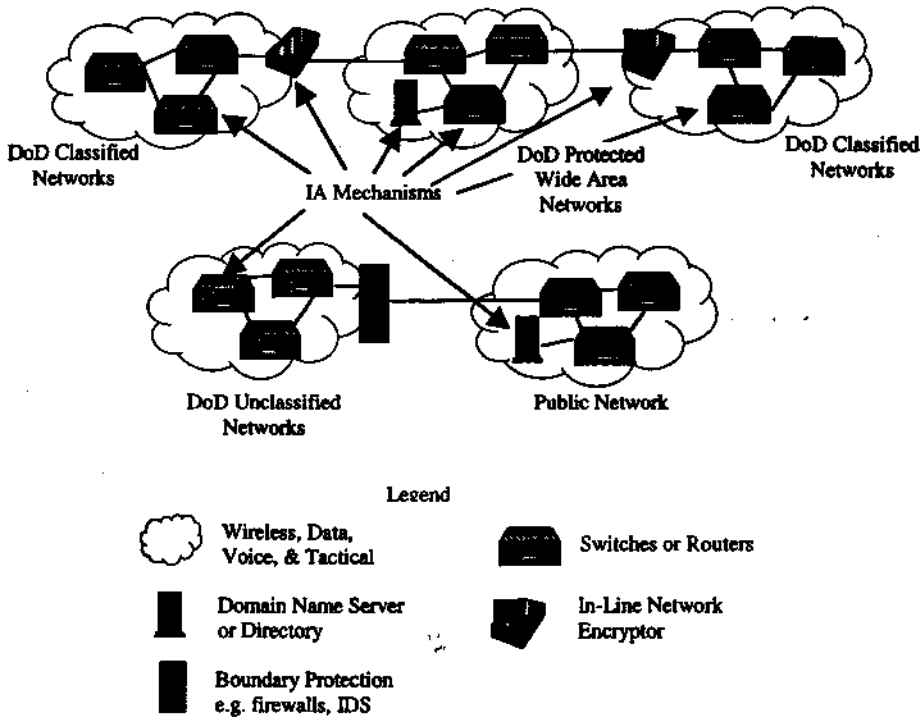

Figure 3-1 Defend the Network

Objectives for Networks
• Ensure that DoD systems and networks follow a consistent architecture. • Ensure that all data within the DoD Enterprise is protected in accordance with its classification and mission criticality. • Ensure that mission critical and mission support networks are protected against denial of service. • Ensure that networks are visible for IA management and monitoring purposes. • Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event. • Ensure that the infrastructure does not conflict with other backbone and enterprise networks or systems.

Table 3-1. Objectives for Network Defense

3.2. Defend the Enclave Boundary: An enclave boundary exists at the point of connection for a LAN or similar network to the service layer. Figure 3-2 depicts a high level view of defend the enclave boundary with suggested placement of IA components and mechanisms (e.g., firewalls and guards). Table 3-2 lists the high level objectives for enclave boundary protection and should be used when designing, implementing or integrating an information technology solution that provides enclave boundary protection. Enclave boundary target environments include: service layer networks, including modem connections; classified LANs within classified WANs (e.g. tunneling information within the SIPRNET); use of virtual private networks on service layer providers; remote enclaves, including remote LANs or systems; laptops that may be connected remotely to different service networks (e.g. Joint Task Force deployments, and high-low transfer and low-to-high transfer.)

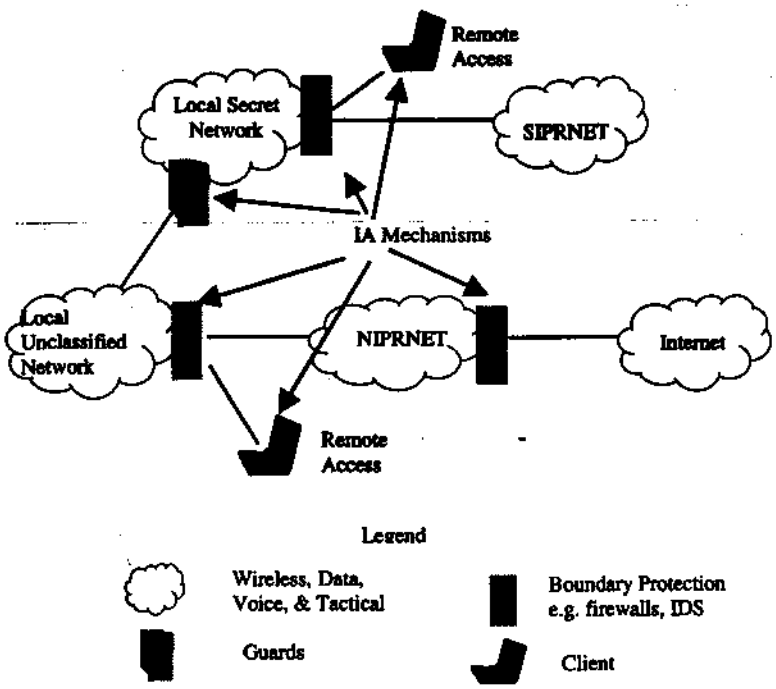

Figure 3-2. Defend the Enclave Boundary

Objectives for the Enclave Boundary
• Ensure that physical and logical enclaves are adequately protected. • Enable dynamic throttling of services due to change in risk posture resulting from changing INFOCONs. • Ensure that systems and networks within protected enclaves maintain acceptable availability and are adequately defended against denial of service intrusions. • Defend against the unauthorized modification or disclosure of data sent outside enclave boundaries. • Provide boundary defenses for those systems within the enclave that cannot defend themselves due to technical or configuration problems. • Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary. • Provide protection against systems and data within the protected enclave being undermined by external systems or forces. • Provide strong authentication of users sending or receiving information from outside their enclave.

Table 3-2 Objectives for Enclave Boundary Defense

3.3. Defend the Computing Environment: Defense of the computing environment is focused on servers and workstations, to include the applications installed on them and the supporting services such intrusion detection which are necessary for the operations of the network. An application is any software written to run on a host, and may include portions of the operating system. Figure 3-3 depicts a high level view of defend the computing environment. Each computing environment (e.g., user workstation, server, system/subsystem) within the enclave requires a minimum of basic protection. Table 3-3 lists high level objectives for computing environment protection. The computing environment includes the end user workstation, both desktop and laptop including peripheral devices; servers including web, application, and file servers; applications such as intrusion detection, e-mail, web, access control and the operating system.

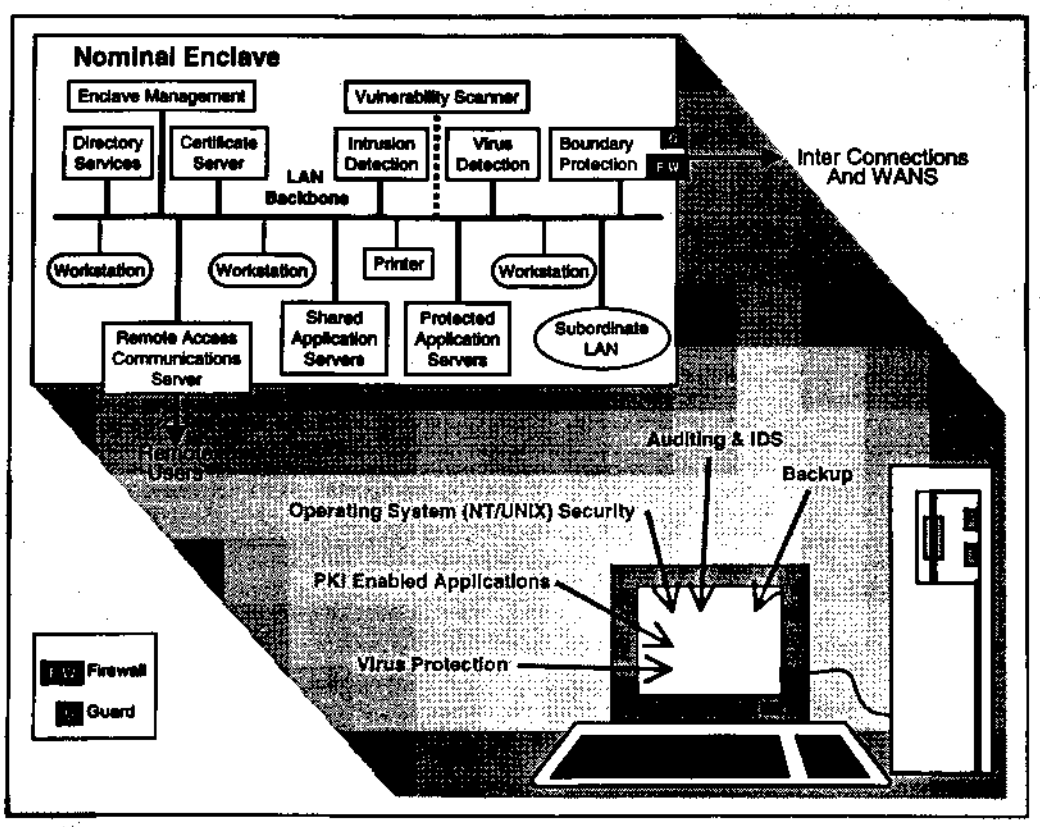

Figure 3-3 Defend the Computing Environment

Objectives for Computing Environment
• Ensure that hosts and applications are adequately defended against denial of service, unauthorized disclosure, and modification of data. • Ensure the confidentiality and integrity of data processed by the host or application whether both internal and external to the enclave. • Defend against the unauthorized use of a host or application. • Ensure that hosts follow secure configuration guidelines and have all appropriate patches applied. • Maintain configuration management of all hosts to track patches and system configuration changes. • Ensure that a variety of applications can be readily integrated with no reduction in security (e.g., to meet the needs of a Joint Task Force). • Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external.

Table 3-3 Objectives for Defense of the Computing Environment

3.4. Establish Supporting Infrastructures: Supporting infrastructures provide the foundation upon which IA mechanisms are used in the network, enclave, and computing environments for securely managing the system and providing security enabled services. The two primary supporting infrastructures are: (1) key management and (2) detect and respond. Table 3-4 lists objectives for supporting infrastructures. Supporting infrastructures provide security services for: networks (e.g. weapons, identify friend or foe, nuclear command and control systems); end-user workstations; servers for web, applications, and files; and, single-use infrastructure machines (e.g. higher level DNS servers, higher-level directory servers). These services apply to both classified and unclassified enclaves.

Objectives for Supporting Infrastructures
• Provide a cryptographic infrastructure that supports key, privilege, and certificate management; and that enables positive identification of individuals utilizing network services. • Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that enables rapid detection and reaction to intrusions and other anomalous events, and that enables operational situation awareness. • Plan execution and reporting requirements for contingencies and reconstitution.

Table 3-4 Objectives for Supporting Infrastructure Capabilities

3.4.1. Key Management Infrastructure: The key management infrastructure provides a common unified process for the secure creation, distribution, and management of the cryptographic products such as asymmetric keys (e.g., PKI) and traditional symmetric keys (e.g., EKMS) that enable security services for the network, enclave, and computing environment. Figures 3-4 and 3-5 depict high level views of the future key management infrastructure architecture and services. KMI-enabled security services such as identification and authentication, access control, integrity, non-repudiation, and confidentiality become increasingly critical as the Department incorporates IA into its electronic systems. Key management provides the common roles and interface processes required to support IA (See DoD KMI documentation).

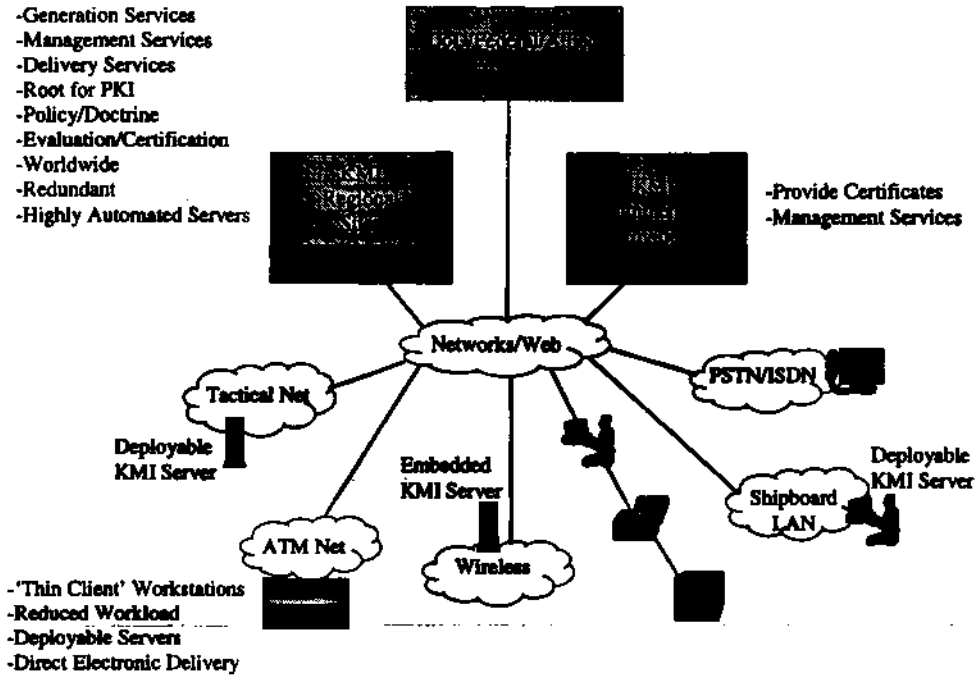

Figure 3-4 Key Management Infrastructure

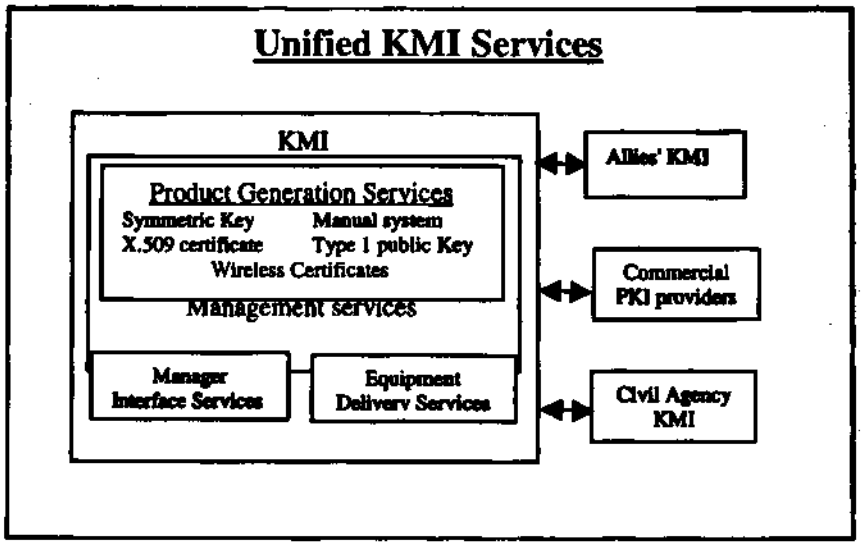

Figure 3-5 Key Management Roles and Processes

3.4.2. Detect and Respond: The cyber battlespace is highly fluid, with operational agility critical to effective defense. The detection, reporting, and response infrastructure enables rapid detection and reaction to intrusions, and enables operational situation awareness and response in support of DoD missions. Local infrastructures support local operations and feed regional and DoD-wide infrastructures, so that DoD can react quickly, regardless of the scale of the intrusion. Figure 3-6 depicts a high level view of the Detect and Respond process

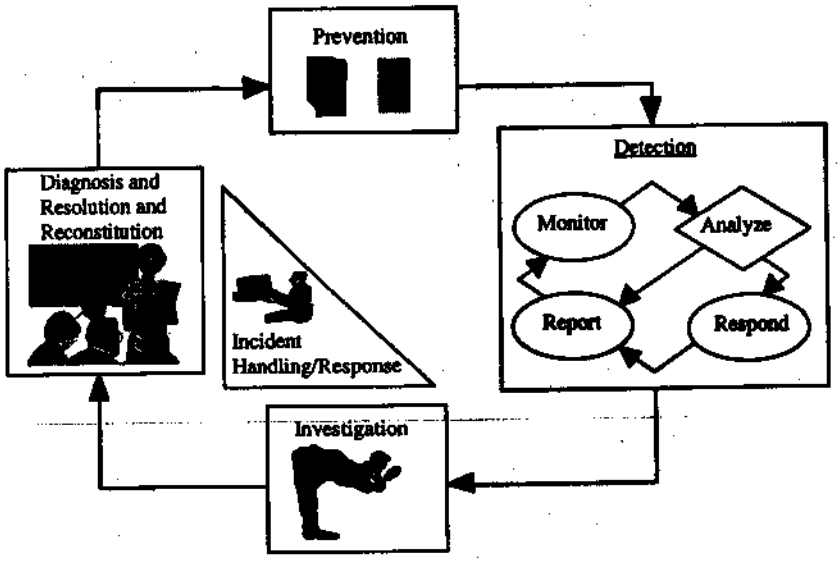

Figure 3-6 Detect and Respond Process

4. Threats and Attacks

Threat is defined as any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, modification of data, or denial of service. Threats may vary based on the motivations and capabilities of adversaries. Threat should be considered from a mission viewpoint as well as from an information processing perspective. Threats must be defined in terms of the threat environment in which the mission will be accomplished. Attack is generally defined as an attempt to gain unauthorized access to an information system's services, resources, or information or the attempt to compromise an information system's integrity, availability, or confidentiality. Factors to consider when determining the threat to a particular solution include: types of attacks, level of access, risk tolerance, expertise, and resources available to the adversary. Attacks can also take many forms. They can include malicious attacks (e.g., virus, worm, Trojan horse, masquerading), unintentional attacks (e.g., malfunction, human error), and physical attacks (e.g., fire, water, battle damage,

power loss). Analysis of potential threats and the countermeasures required to maintain the appropriate confidentiality, integrity, and availability of the information is required to define the best practices to mitigate risk and support defense-in-depth. Table 4-1 provides common threat considerations and Table 4-2 provides categories of attacks. All these factors should be considered when designing a system.

Common Threat Considerations
• Insider intrusions - both human error and malicious
• Network based attacks both systematic and random
• Jamming of networks both malicious and inadvertent
• Flooding
• Theft of service
• Disruption of network management communications and services
• Unauthorized access to network operations and management
• Unauthorized intrusions by remote operators
• Malicious software developers and software
• Malicious hardware developers and hardware
• Overrun by adversaries
• Unauthorized access by others with physical access

Table 4-1 Common Threat Considerations

- **Passive Intercept Attacks** – include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing identification numbers and passwords. Passive intercept of network operations can give adversaries indications and warnings of impending actions.
- **Network-Based Attacks** – include attempts to circumvent or break security features, introduce malicious code or to steal or modify information. These include attacks mounted against a network backbone, exploitation of information in transit, electronic penetrations into an enclave, or attacks on an authorized remote user when she attempts to connect to an enclave.
- **Close-in Network-Based Attacks** – attempt to execute network-based attacks to penetrate an enclave's protection where the adversary gains access at a point inside the network and infrastructure protection boundary.
- **Insider Attacks** – are performed by individuals who are authorized physical access to the system or network or have authorized electronic access to that system or network. Malicious insiders have the intent to eavesdrop, steal, or damage information, or to deny access to other authorized users. Non-malicious attacks (typically resulting from carelessness or lack of knowledge) are also considered threats since their actions may have security consequences.
- **Hardware/Software Distribution Attacks** – focus on the malicious modification of hardware or software at the factory or modification or substitution during distribution.

Table 4-2 Categories of Attacks

5 Levels of Robustness

5.1. Robustness describes the strength of mechanism (e.g., the strength of a cryptographic algorithm) and design assurance (i.e. confidence measures taken to ensure proper mechanism implementation) for a technical IA solution. Technical IA solutions in the defense-in-depth strategy will be at one of three defined levels of robustness: high, medium, or basic, corresponding to the level of concern assigned to the system. Designating levels indicates a degree of robustness of the solution. Evaluation Assurance Level (EAL) levels, defined in the International Common Criteria, and classes of certificates, defined in the DoD Certificate Policy, indicate a degree of confidence in the security attributes of the products they relate to. As security mechanisms improve over the years, the robustness of security products should also improve, and more robust products can be incorporated in security solutions. The more robust a particular security attribute is, the greater the level of protection it provides to the security services it supports. Assigning levels of robustness for integrity, availability and confidentiality for all DoD information systems is another means for ensuring the most cost effective and best use of IA solutions, including COTS solutions. When implementing IA solutions, they will be at a designated robustness level commensurate with the level of concern, except where noted. It is also possible to use non-technical measures to achieve protection requirements dictated by the level of concern. For example, physical isolation and protection of a network can be used to provide confidentiality. In these cases, the technical solution requirement may be reduced or eliminated. The three levels of robustness discussed below are based on the robustness strategy presented in the IATF. It should be noted that today's technology could support development of more stringent protection and rigorous security countermeasures, however, development costs would far exceed acceptable budget limits. Therefore, the term high robustness, used here, is relative to the other levels of robustness, including those of the IATF robustness strategy, and does not indicate the best that could be developed in an unrestrained environment. The three levels of technical robustness solutions are described in the following sub-paragraphs.

5.1.1. High robustness security services and mechanisms provide the most stringent protection and rigorous security countermeasures. High robustness solutions require all of the following:

- NSA-certified Type 1 cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash
- NSA Type 1 cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication)
- Key Management:
  - For symmetric key, NSA-approved key management (production, control and distribution.)
  - For asymmetric key, Class 5 PKI certificates and hardware security tokens that protect the user's private key and crypto-algorithm implementation.

- High assurance security design, such as specified by NSA or the International Common Criteria (CC) at a minimum an Evaluated Assurance Level (EAL) greater than 4.
- Products evaluated and certified by NSA.

5.1.2. Medium robustness security services and mechanisms provide for additional safeguards above the DoD minimum. Medium robustness solutions require, at a minimum, all of the following:

- NIST FIPS validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table 5-4)
- NIST cryptographically authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication)
- Key Management:
  - For symmetric key, NSA-approved key management (production, control and distribution.)
  - For asymmetric key, Class 4 PKI certificates and hardware security tokens that protect the user's private key
- Good assurance security design such as specified in CC as EAL3 or greater
- Solutions evaluated and validated under the Common Criteria Evaluation validation scheme or NSA
- Solutions for National Security Systems approved by NSA

5.1.3. Basic robustness solutions are equivalent to good commercial practice. Basic robustness require, at a minimum, all of the following:

- NIST FIPS validated cryptography (algorithms and implementation) for encryption, key exchange, digital signature, and hash (see algorithms at Table 5-4)
- Authenticated access control (e.g., digital signature, public key cryptography based, challenge/response identification and authentication or pre-placed keying material)
- Key Management:
  - For symmetric key, NIST-approved key management (production, control and distribution.)
  - For asymmetric key, Class 3 PKI certificates or pre-placed keying material. See reference (p) for policy on migration to Class 4 certificates and software tokens (private keys held in software on the user's workstation.)
- CC EAL 1 or greater assurance
- Solutions evaluated and validated under the NIAP Common Criteria Evaluation Validation Scheme or NSA

5.2. While paragraph 5.1. focuses on the robustness of individual security services and mechanisms, the robustness of a network solution must be considered in the context of defense-in-depth (see section 3) and the threat environment in which the system operates. For instance, a system operating on a protected backbone between secure enclaves may not require additional mechanisms for authentication and access control. In addition, if community of interest separation is provided through encryption, it will require less robust solutions.

5.3. The tables below are tools for use in a disciplined system security engineering approach for building or replacing systems. They cover the major defense in depth areas but are not all-inclusive for every system requirement and should not be used as a substitute for good systems security engineering. The robustness indicated is the minimum that should be considered for the defense in depth application in the environment listed. However, more robust solutions should always be considered during the in-depth security analysis of system requirements. In addition, as information assurance technology improves, and systems are replaced or upgraded, higher robustness solutions should always be considered.

5.3.1. Availability ensures that the resources and data are in place, at the time and in the form needed by the user. Availability can be enhanced by access control, which limits access to authorized users only. Integrity ensures that data has not been altered or destroyed and is achieved through the use of digital signatures or keyed hash schemes. Non-repudiation provides the ability to prove to a third party that an entity did indeed participate in a communication. Non-repudiation is provided by the authenticating characteristics of digital signatures. Minimum robustness requirements for availability, integrity, and non-repudiation are shown in Table 5-1.

Security Service	**Level of Concern/Robustness**		
	High	**Medium**	**Basic**
Availability		Mission Critical over an unencrypted network.	1. Mission support and Administrative over any network. 2. Mission Critical over an encrypted network.
Integrity, Non-repudiation		1. Mission Critical over an unencrypted network. 2. Network Management commands over an unencrypted network.	1. Mission Critical over an encrypted network. 2. Mission support and Administrative over any network. 3. Network Management commands over an encrypted network.

Table 5-1 Security Services Robustness

5.3.2. Access Control is used to limit access to networked resources (hardware and software) and data (stored and communicated). The main elements of access control are identification and authentication (I&A) and authorization. Passwords, tokens, and certificates are used to achieve authenticated access control. Table 5-2 gives examples of minimum robustness requirements for access control mechanisms in particular situations.

Defense in Depth Application examples	**Level of Concern/Robustness for Access Control**	
	Encrypted and/or Physically Isolated Network	**Unencrypted or not Physically isolated Network**
Defend the Network		
Access to DoD Network Management Centers and all Network Management control commands to managed GIG components (e.g. routers, switches), as well as inter-element commands (e.g. router table propagation)	Basic	Medium
Defend the Enclave		
All interconnections between Enclaves or LANs operating at different classification levels, (e.g. TS to Secret, Secret to Unclassified) or between U.S, and foreign nation systems or networks will only be through a well-defined and controlled gateway. (NOTE: Connection between different classification levels allow lower classified or unclassified data from the higher classified system to be moved to the lower classified or unclassified system (e.g., unclassified data on a secret system to an unclassified system). In addition, unclassified data from an unclassified system can be moved to a classified system with the use of a well-defined and controlled gateway.	Medium + (The level of robustness for this case, which is also know as a high assurance guard, is medium, however additional design assurance is required and must have an EAL greater than 4.)	Medium + (The level of robustness for this case, which is also know as a high assurance guard, is medium, however additional design assurance is required and must have an EAL greater than 4.)

All boundaries between Enclaves at the same sensitivity level and the WAN will be protected	Basic	Basic- for mission support and administrative information Medium- for Mission critical
(NOTE: All gateways at boundaries between Enclaves and WAN will contain an intrusion detection / attack sensing and warning capability. All interconnections between Enclaves or LANs operating at different classification levels should be designed and analyzed to reduce covert channels)		
Defend the Computing Environment	**Encrypted and/or Physically Isolated Network**	**Unencrypted or not Physically isolated Network**
User Logon to a workstation to gain access to network resources	Basic	Basic
User access to servers (e.g. Web servers, database servers, file servers) or other components storing Special Compartmented, Special Access, or other Mission Critical information, will use authenticated access.	Basic	Medium
User accesses to servers (e.g. Web servers, database servers, file servers) or other components storing mission support or administrative, will use authenticated access.	Basic	Basic
All Network Management control commands to managed GIG components (e.g. routers, switches), as well as inter-element commands (e.g. router table propagation) in the Enclave will employ authentication.	Basic	Medium
All Mission Critical, Mission Support and Administrative transactions, to include individual (non-organizational) e-mail and e-commerce, will be secured with a digital signature.	Basic	Basic- for mission support and administrative information Medium- for Mission Critical information

Table 5-2 Access Control Robustness Examples

5.3.3. Encryption is a procedure to convert plain text into cipher text. Within DoD it is used for purposes of:

5.3.3.1. Confidentiality: To ensure that information is not made available or disclosed to unauthorized individuals, entities, or processes.

5.3.3.2. Data Separation: To ensure that information of different classifications sharing the same transport (transmission) media are not co-mingled.

5.3.3.3. Privacy: To ensure that information at the same classification level is kept separate based on need-to-know.

5.3.4. Table 5-3 provides robustness guidance for data encryption robustness. Note that when information is encrypted for the purposes of data separation or privacy, it is always tunneled through a network that is also encrypted for confidentiality.

Purpose of Encryption	Data classification / Network Type	Minimum Robustness of Algorithm
Confidentiality	TS through Secret	High
	TS through Commercial	High
	Secret through Commercial	High
	Unclassified Sensitive through Commercial	Basic
Data Separation	Secret through TS	Medium
	U through TS	Medium
	U through Secret	Medium
Privacy	TS through TS	Basic
	Secret through Secret	Basic
	Unclassified through Unclassified Sensitive	Basic

Table 5-3 Data Encryption Robustness

5.3.5. Cryptographic functions include encryption, hash, signature and key exchange algorithms. These algorithms are used to protect the confidentiality and/or integrity of information. Table 5-4 lists currently available algorithms. It includes algorithms that are often encountered in commercial products primarily for reference purposes. The number of bits or the length of the cryptographic key used in the algorithm and the design assurance of the algorithm are directly related to its robustness and will determine whether the NIST certified algorithms listed in Table 5-4 are basic or medium robustness. Within the Department of Defense, only NSA or NIST certified cryptographic algorithms may be used unless otherwise authorized. See Chapter 4 of the IATF (http://www.iatf.net) for a detailed description of algorithm robustness.

Algorithm	Commercially Available (Reference)	NIST Certified Basic/Medium Robustness	NSA Certified High Robustness
Encryption Algorithm	RC4 RC5 IDEA Blowfish	AEA DES* SKIPJACK	Contact NSA
Hash Algorithm	MD5 New standards as available	SHA 1 New standards as available	Contact NSA
Signature Algorithm	RSA EDSA	DSA	Contact NSA
Key Encryption Algorithm	RSA DH	KEA	Contact NSA
AEA- Advanced Encryption Algorithm DES- Digital Encryption Standard DH- Diffie-Hellman DSA- Digital Signature Algorithm EDSA- Elliptic Digital Signature Algorithm Hash- One way mathematical operation		IDEA- International Data Encryption Algorithm KEA- Key Encryption Algorithm MD5- Message Digest 5 RSA- Rivest-Shamir-Adleman SHA- Secure Hash Algorithm	

* - 3DES is currently recognized as a de facto standard, but has not been NIST Certified.

Table 5-4 Algorithm Robustness Examples

6. Non-Technical Countermeasures. The defense in depth strategy relies on both technical and non-technical countermeasures as equal elements to establish and maintain an acceptable IA posture across the DoD. Non-technical countermeasures are discussed below.

6.1.Personnel Security: Personnel security is an integral part of the overall Information Assurance program. Specific requirements for personnel assigned to Information Assurance jobs can be found in DoD Regulation 5200.2R, "Personnel Security Program".

6.2. Physical Security: Physical Security is the action taken to protect DoD information technology resources (e.g. installations, personnel, equipment, electronic media, documents, etc.) from damage, loss, theft, or unauthorized physical access. Specific guidance can be found in DoD Regulation 5200.8, "Security of Military Installations and Resources."

6.3 Procedural Security: Procedural Security is an integral part of the overall Information Assurance environment and supports the concepts of defense-in-depth. Procedural security measures both complement technical security measures, and can provide alternatives to technical security means when risk analysis indicates the use of procedures does not increase the overall risk to a system or network. Procedural Security provides the necessary actions, controls, processes, and plans to ensure continuous operation of a system or network within an accredited security posture, and is site and task dependent. Site security procedures shall be developed to supplement the security features of the hardware, software and firmware of information technology resources, to include such standardized processes as security training, user access control, media labeling and classified material handling.

6.4. Security Training, Education and Certification. Security education, training, and awareness are essential to a successful IA program. Employees who are informed of applicable organizational policies and procedures can be expected to act effectively to ensure the security of system resources. General users require different training than those employees with specialized responsibilities. Minimum IA training requirements to support defense-in-depth can be found in joint USD (P&R) and ASD (C3I) guidance.

6.5. Marking and Labeling

6.5.1. Storage Media: Information storage media used in a classified information system is classified at the level of that information system. Information storage media will have external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. ISSO's and SA's shall identify the removable storage media to be used with a system

6.5.1.1. Removable media shall be marked, physically controlled, and safeguarded in the manner prescribed for the highest classification level ever recorded on it until destroyed or sanitized using approved processes.

6.5.1.2. Non-removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. If it is difficult to mark the non-removable media itself, the labels described below may be placed in a readily visible position on the cabinet enclosing the media.

6.5.2. Marking Hardware Components. Procedures shall be implemented to ensure that all components of an IS, including input/output devices that retain information, terminals, standalone microprocessors, and word processors used as terminals, bear a conspicuous, external label. This label shall state the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may consist of permanent markings on the component or a sign placed on the terminal.

6.5.3. Marking Human-Readable Output.

6.5.3.1. Human-readable output shall be marked appropriately, on each human-readable page, screen, or equivalent (e.g., the proper classification must appear on each classified microfiche *and* on each page of text on the fiche).

6.5.3.2. Warning Notices: All individuals attempting access to DoD information systems shall be provided sufficient notice that use of official DoD information systems or networks constitutes consent to monitoring. Adequate warning shall be provided by clearly displaying a legally approved DoD warning notice. At a minimum, the warning banners on computer systems shall be displayed to the user upon initial entry/login to system, network, local, and remote resources. Acceptance of the banner warning screen shall constitute consent to monitoring.

6.6. Standard Operating Procedures: Consistent, clearly documented operating procedures for both system configuration and operational use are key to ensuring information assurance. Procedures should define deployment of the system, system configuration, day to day operations for both the system administrator and user, as well as how to respond to real or perceived attempts to violate system security. All DoD information systems and networks shall include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment.

6.7. Incident Reporting and Response: In addition to protective measures designed into information systems and architectures, sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of DoD operations.

6.7.1. Incident Reporting: All DoD organizations shall promptly report incidents via their appropriate chain of command. Types of incidents that will be reported include:

6.7.1.1. Intrusion: Unauthorized access to an information system.

6.7.1.2. Denial of Service Attacks: Actions which prevent any part of an automated information system from functioning in accordance with its intended purpose, to include any action which causes the unauthorized destruction, modification, or delay of service.

6.7.1.3 Malicious Logic: Hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose, such as a virus or Trojan horse.

6.7.1.4. Probe: In information operations, any attempt to gather information about an automated information system or its users online.

6.7.2. Computer Incident Response: In accordance with the JTF-CND Concept of Operations dated December 1998, the JTF CND, serves as the DoD primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten DoD information systems and networks. The JTF CND will collaborate and coordinate DoD efforts with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

6.7.3. COMSEC Material Incident Reporting: Incidents involving the compromise or the suspected compromise of COMSEC material or incidents that warrant further investigation shall be reported in accordance with NSTISSI 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated August 1997.

6.8. Assessments

6.8.1. Vulnerability Assessments: Vulnerability assessments identify vulnerabilities in an operational environment and validate a particular site's overall security posture and degree of system integration and usually provide recommendations on ways to address shortcomings. Types of assessments include, but are not limited to:

6.8.1.1. Monitoring: Monitoring is an on-line assessment to better understand the vulnerability of DoD systems.

6.8.1.2 On-Line Surveys: On-line surveys conducted by Services and Defense agencies help DoD commands identify vulnerabilities on assigned and joint systems.

6.8.2 Commands may request more detailed on-site assistance (e.g., on-site assessments and ISSE surveys) to better understand their vulnerabilities.

6.8.3. Red Team Operations: Red Team operations may be employed to validate existing IA protections and to exercise standard operating procedures and tactics to evaluate vulnerabilities.

6.9. Risk Management

6.9.1. Risk management is the discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment. Risk management is an important aspect of information assurance and defense-in-depth.

6.9.2. The risk management process identifies assets to be protected, potential threats and vulnerabilities, and countermeasures and safeguards that can eliminate vulnerabilities or reduce them to levels acceptable for IS accreditation. Risk management is based on careful identification and evaluation of the threats and vulnerabilities that apply to a given IS and its operational environment.

6.9.3. Risk management is relevant to the entire life cycle of an IS. During IS development, security countermeasures are chosen. During IS implementation and operation, the effectiveness of in-place countermeasures is reconfirmed, and the effect of current threat conditions on system security is assessed to determine if additional countermeasures are needed to sustain the accredited IS's security. In scheduling risk management activities and designating resources, careful consideration should be given to Certification and Accreditation (C&A) goals and milestones. Associated risks can then be assessed and corrective action taken for unacceptable risks. Risk management requires the routine tracking and evaluation of the security state of an IS. The risk management process includes:

6.9.3.1. Analysis of the threats to and vulnerabilities of an information system, as well as of the potential impact that losing the system's information or capabilities would have on national security. This analysis forms a basis for identifying appropriate and cost-effective countermeasures.

6.9.3.2. Risk mitigation. Analysis of trade-offs among alternative sets of possible safeguards.

6.9.3.3. Residual risk determination. Identification of the risk remaining after applying safeguards.

6.9.3.4. Acceptable level of risk. Judicious and carefully considered assessment by the appropriate DAA that the residual risk inherent in operating the IS after implementing all proposed security features is acceptable.

6.9.3.5. A reactive or responsive risk management process. To facilitate investigation of, and response to, incidents.

6.9.4. The risk management process applies to all layers of the defense-in-depth strategy and the transition points between defense-in-depth layers. Interconnected systems pose risks that must be mitigated, in part, by further management processes

6.9.4.1. Configuration Management: Configuration management identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle. Proper configuration management can substantially reduce and sometimes eliminate the need for costly complete re-accreditation. Appropriate levels of configuration management shall be established to maintain the accredited security posture. The security impact of each change or modification to an information system or site configuration shall be assessed against the security requirements and the accreditation conditions issued by the DAA.

6.9.4.2. Data Management: The increasing reliance on distributed, interconnected information systems negates many of the data protection mechanisms built in to traditional "system high" networks and requires additional safeguards to protect DoD information from both unauthorized users and from authorized users without a need to know.

6.9.4.3. Requirements Management: For specific systems security requirements for passwords, marking guidance and implementation, account management, and operating systems security requirements, please refer to the Defense Information Infrastructure Common Operating Environment (DII COE) Software Requirements Specification for security version 4.0 dated 20 October 1998.

6.10 System Security Policy: An Information System Security Policy (ISSP) shall be developed and maintained for every DoD organization employing information technology resources and for each information system used within the DoD. The ISSP shall identify the security requirements, objectives and policies implemented to safeguard the site or system in a prescribed operational configuration, to include requirements for system redundancy and data backup and risk management decisions. Contingency plans will be developed and tested to prepare for emergency response, backup operations, and post-disaster recovery. This policy document will become part of the SSAA required by the DISTCAP.