USAWC STRATEGY RESEARCH PROJECT

A WAY TO OPERATIONALIZE THE DOD'S CRITICAL INFRASTRUCTURE PROTECTION PROGRAM USING INFORMATION ASSURANCE POLICIES AND TECHNOLOGIES

by

Mr. Arthur R. Friedman
National Security Agency

Dr. James B. Bartholomees
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Way to Operationalize the DOD's Critical Infrastructure Protection Program Using Information Assurance Policies and Technologies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Arthur Friedman**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**34**	

ABSTRACT

AUTHOR: Arthur R. Friedman

TITLE: A Way To Operationalize The DoD's Critical Infrastructure Protection Program Using Information Assurance Policies And Technologies

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 34 CLASSIFICATION: Unclassified

The Department of Defense (DoD) Defense Critical Infrastructure Protection Program has recently reorganized under the Office of the Assistant Secretary of Defense for Homeland Defense under the Under Secretary of Defense for Policy. Requirements have been set forth in DoDD 3020.ff, Defense Critical Infrastructure, which is in final coordination and is anticipated to be published later this fiscal year. This policy states that Defense Critical Infrastructure and non-DoD infrastructures are essential to planning, mobilizing, deploying, and sustaining military operations within the U.S. as well as globally, shall be available when required. Today's Combatant Commanders do not have the ability to quickly and efficiently share information that identifies critical infrastructure assets and single points of failure to prevent physical or cyber attacks from impairing the Global Information Grid. The intent of this paper is to provide a construct to Operationalize the DoD's Critical Infrastructure Protection Program through the use of Information Assurance policies, methodologies, and technologies, and to identify strategic implications of vulnerabilities to the Combatant Commander and supporting agencies.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I want to take this opportunity to express my appreciation to several individuals who contributed to the development of this paper during a thought-provoking time in my career while attending the U.S. Army War College.

Mr. William N. Bryan and Mr. Daniel Mathias from the Office of the Assistant Secretary of Defense for Homeland Defense and Mr. Larry Huffman and Mr. Hector Ruiz from the Defense Information Systems Agency were all very supportive in providing their leadership and encouragement in addressing new and challenging ways to operationalize the Defense Critical Infrastructure Protection Program.

l want to thank a number of individuals that provided specific comments and advice for the development of this paper. These individuals include Ms. Kathleen Young, Defense Program Office for Mission Assurance; Ms. Lesley Painchaud, Alion, Inc.; Ms. Joan Grewe and Mr. Daniel Wagner, National Security Research, Inc.; Prof. Cynthia E. Ayers, U.S. Army War College; and my faculty instructors at the U.S. Army War College, Dr. James B. Bartholomees and Dr. William G. Pierce.

LIST OF ILLUSTRATIONS

A WAY TO OPERATIONALIZE THE DOD'S CRITICAL INFRASTRUCTURE PROTECTION PROGRAM USING INFORMATION ASSURANCE POLICIES AND TECHNOLOGIES

> "The world changed on September 11, 2001. We learned that a threat that gathers on the other side of the earth can strike our own citizens. It's an important lesson; one we can never forget. Oceans no longer protect America from the dangers of this world. We're protected by daily vigilance at home. And we will be protected by resolute and decisive action against threats abroad."
>
> - President George W. Bush
> September 17, 2002

BACKGROUND

The Department of Defense (DoD) continues to increase its dependence on commercial resources to assist in implementing military plans and executing its missions. In light of this situation, the DoD Defense Critical Infrastructure Protection (DCIP) strategy expects for military operations to become increasingly dependent on supporting infrastructure assets. With the dependence on these critical assets and the growth in outsourcing and privatization activities in the United States and overseas, the military will continue to make risk management decisions with respect to the level of investment needed to protect the critical infrastructure.

The Critical Infrastructure Protection (CIP) Program was initially conceived at the national level and discussed in a report issued by the President's Commission on Critical Infrastructure Protection as a risk management strategy. "It was for just this purpose that President Clinton called into being the President's Commission on Critical Infrastructure Protection in July 1996. In the fifteen months since its creation, the Commission – drawn from the federal government and the private sector – has thoroughly reviewed the vulnerabilities and threats facing our infrastructures."[1] This strategy was designed to provide processes, tools, and methodologies for making economic decisions about the types of protection or security that will be required to assure the continued availability of our critical assets. Even though DoD's CIP Program was established during the Clinton administration as a result of Presidential Decision Directive 63 (PDD 63),[2] the policies and funding were lacking for this program to be effective. Following the September 11, 2001 attacks on the World Trade Center and the Pentagon, however, senior government officials realized that the DoD DCIP should become part of the national emergency

management planning and decision making process, and recommended the identification of funding specifically for the protection of the Defense Critical Infrastructure.[3]

On May 17, 2001, the Honorable Linton Wells II, Acting Assistant Secretary of Defense for Command, Control, Communications and Intelligence and DoD Chief Information Officer, testified before the House Armed Services Committee on the topic of Information Assurance (IA).[4] The testimony described a strategy entitled "Defense-in-Depth" and highlighted a GAO report entitled *Information Security: Challenges to Improving DoD's Incident Response Capabilities (GAO-01-341)*, but did not describe the relevance of using this strategy in supporting the principles of DCIP. "Defense-in-Depth is mandated by DoD as the main IA implementation strategy to be used to protect national security systems and information."[5] DoD policy makers describe Defense-in-Depth as:

> . . . the DoD approach for establishing an adequate information assurance (IA) posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among information technology assets; and the selection of IA solutions based on their relative level of robustness.[6]

On May 10, 2004, the Assistant Secretary of Defense for Homeland Defense, Paul McHale, submitted a final coordination draft of Department of Defense Directive 3020.ff, entitled *Defense Critical Infrastructure*. This directive establishes policy and assigns responsibility for the Defense Critical Infrastructure activities, which requires the DoD to:

"Ensure both DoD and non-DoD infrastructures essential to planning, mobilizing, deploying, executing and sustaining United States military operations on a global basis are available when required.

Address Defense Critical Infrastructure vulnerabilities based on risk management decisions made by responsible authorities.

Coordinate with other federal agencies, state and local governments, the private sector, and equivalent foreign entities as required to ensure the continuity of Defense Critical Infrastructures.

Establish a DCIP program to identify, prioritize, and coordinate the protection of critical assets.

Elevate the awareness of and promote DCIP through a variety of activities, such as information sharing and cooperative arrangements with the private sector, as well as other

federal departments, state and local governments, and allied/friendly foreign governments, as necessary."[7]

The DCIP strategy is designed to provide DoD with improved mission assurance capabilities and help manage risk for DoD's critical infrastructure assets. In that regard, the draft DoD Directive 3020.ff is a significant improvement over previous published policies; however, the proposed draft still lacks guidance in a number of technical disciplines that incorporate the Defense Information Assurance Program (DIAP) and Defense-in-Depth strategy.

IA is critical to the military's ability to conduct Information Operations, and is a major component of DoD Critical Infrastructure Protection. Greater coordination with the DIAP is essential to ensure that DoD Directive 3020.ff adopts the concepts of layered protection offered through IA practices and provides improved situational awareness to the Combatant Commander. This can be achieved by operationalizing the DCIP Program. The concept of operationalizing the DCIP Program has been discussed at all levels of command; however, there has been no agreed upon approach. The approach presented in this paper describes the use of Information Assurance policies, methodologies and technologies to operationalize the DCIP Program and build on the concept of the Global Network Operations Command and Control process. The concept consists of integrating multiple sources of data, both new and existing, and providing this data in a format that is useful to the Combatant Commander and supporting agencies.

The approach to operationalizing the DCIP Program is based on a three-point strategy that includes: (1) expanding the existing network operations framework used by the Computer Network Defense (CND) community, (2) integrating DoD's Defense-in-Depth concepts and Information Assurance policy and technology, and (3) using information collected from existing technical assessment programs to support DCIP. The Combatant Commander has access to the results of the assessment programs; however, integration of all collected data to protect the DoD critical infrastructure has not been accomplished, nor is there a current plan to do so. Many Combatant Command staffs are not even aware of the vulnerabilities identified by IA tools and DCIP data that currently exist on multiple databases to assist them when making deployment decisions.

For example, the DoD Computer Emergency Response Team (CERT) publishes Information Assurance Vulnerability Alerts (IAVAs) to notify system administrators throughout the DoD to correct a software deficiency or install approved software patches. By taking swift, corrective action, the Combatant Commander can have a high degree of assurance that the

information systems needed to make command and control decisions will be available when required. IAVAs can prevent those who exploit network vulnerabilities from destroying or denying access to critical data that resides on the Global Information Grid (GIG), which is a major critical asset in DoD's infrastructure. Attacks on any one of hundreds of critical assets may have cascading effects that can impact the availability of transportation, medical, and logistical support. To protect these critical assets and ensure that the Combatant Commander has the resources needed to mobilize, it is essential to operationalize the protection of DoD's critical infrastructure.

Operationalizing the DCIP Program is much more complicated than publishing new policies (such as DoD Directive 3020.ff) or creating a command and control center to collect and disseminate infrastructure vulnerabilities. The concept consists of integrating multiple sources of data, both new and existing, and providing this data in a format that is useful to the Combatant Commander and supporting agencies. Existing assessment programs and operations centers will be challenged to embrace and integrate this important mission into existing operations, but the access to DCIP information can be crucial to the process of assessing the readiness levels of support elements needed to accomplish the Combatant Commander's mission.

NETWORK OPERATIONS FRAMEWORK SUPPORTING DCIP

Operationalizing the DCIP Program and integrating improved decision support tools will help improve situational awareness regarding the status of all defense critical assets, and provide capabilities to analyze the impacts caused by loss or degradation of those assets. Before the Combatant Command staffs can use relevant DCIP data to determine their readiness levels, the framework of network operations (NetOps)[8] should also be expanded to improve coordination within the DoD, federal agencies, state and local governments, the private sector, and equivalent foreign entities as required, to ensure the continuity of Defense Critical Infrastructures. "NetOps is the operational construct that the Commander, US Strategic Command (CDRUSSTRATCOM) will use to operate and defend the Global Information Grid (GIG). The goal of NetOps is to provide assured Net-centric services across strategic, operational and tactical boundaries in support of DOD's full spectrum of war fighting, intelligence and business missions. NetOps 'Service Assurance' goals include: Assured system and network availability, Assured information protection, and Assured information delivery."[9] The NetOps construct can be used to monitor and analyze network information obtained during the examination of critical infrastructure assets and GIG interdependencies. The NetOps command

and control (C2) process should be expanded to include sharing information with other C2 processes.

The Mission Assurance Support Center (MASC),[10] which is an independent operations center, is not integrated into the Global NetOps C2 process. The Global NetOps C2 process includes people and organizations at the Strategic level, specifically, representatives from the Chairman, Joint Staff; National Military Command Center (NMCC); USSTRATCOM; Joint Task Force – Global Network Operations (JTF-GNO); Global NetOps Center (GNC); National Security Incident Response Center (NSIRC);[11] Functional Combatant Commands; and Service/Agency Headquarters. This paper recommends that the MASC, which can also have strategic level responsibilities in support of the CND mission helping the Combatant Commanders understand the critical assets needed to conduct their missions, be included in this NetOps command and control structure. Figure 1 graphically portrays the command and control relationships for Global NetOps. This figure has been modified to show an informal reporting relationship with the MASC.

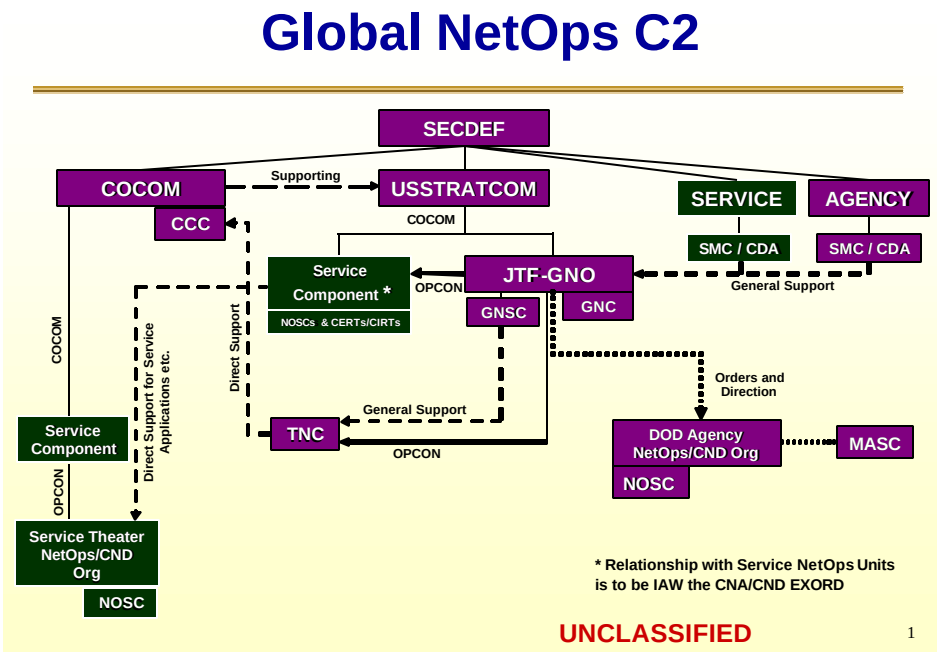

FIGURE 1: GLOBAL NETOPS COMMAND AND CONTROL[12]

Existing tactics, techniques and procedures (TTPs) are not yet sufficiently developed to address the details of how vulnerability information can be integrated into the Global NetOps C2 process to protect the GIG from physical and cyber attack, but the MASC could play an important role in cataloging vulnerabilities and disseminating this information to the JTF-GNO for their assessment of the overall threat to the GIG. This can be accomplished by expanding the scope of the MASC's responsibilities in support of the Global NetOps C2 mission, and adding a capability to provide value-added information concerning the readiness and posture of critical GIG assets.

The GIG is designed to provide an end-to-end set of information services, NetOps capabilities, associated processes, and people to manage and provide the right information to the right user at the right time with appropriate protection across all DoD war-fighting, intelligence, and business domains. The current net-centric transformation[13] initiative underway at DoD is driving the Defense Information Systems Agency (DISA) to take on a greater operational role by incorporating the Defense Critical Infrastructure requirements into the Global NetOps C2 process. DISA, having jointly designed, developed and fielded the Global NetOps C2 process with JTF-GNO, is currently the GIG sector lead for the DCIP Program; however, its involvement in supporting the Defense Program Office – Mission Assurance (DPO-MA) is limited. DISA has the expertise to offer in-depth systems engineering support as well as assistance in identifying critical GIG assets. By incorporating some of DISA's major initiatives such as the Net-Centric Enterprise Services (NCES)[14] and GIG Bandwidth Expansion (BE)[15] programs into the DCIP strategy and its Enterprise Architecture, the DoD will come closer to achieving its goal of Mission Assurance. This increased role for DISA will also impact its indirect support to the DCIP strategy, which will require closer coordination with the DPO-MA.

INTEGRATING DEFENSE-IN-DEPTH INTO DCIP

There are several existing DoD initiatives that have the potential of being utilized in the protection of DoD infrastructure and that could also be considered for broader national security applications. These include:

Information Operations Condition (INFOCON) levels

Computer Network Defense Service (CNDS) Certification

National Security and Emergency Preparedness (NS/EP).

Two of the above initiatives (INFOCON levels and CNDS Certification) fall under the CND umbrella, which is now the responsibility of the USSTRATCOM Combatant Commander. These programs need to be addressed in greater detail in DoD Directive 3020.ff. The third initiative, NS/EP, is managed by the National Communications System (NCS),[16] formerly part of the DoD and now part of the Department of Homeland Security (DHS).

INFORMATION OPERATIONS CONDITION

INFOCON levels[17] were established for the DoD as a structured, coordinated approach for defense against adversarial attacks on DoD computers and telecommunications. INFOCON is a system of indications and warning that has long been practiced by the U.S. intelligence community for military operations. In today's network-centric environment there is greater risk to all users that access the GIG. Users must plan to operate in an environment where risk is shared by all commands that access the GIG. Unlike most other military operations a successful network intrusion in one area of responsibility (AOR) may, in many cases, facilitate access into other AORs. This reality necessitates a common understanding of the situation and responses associated with the declared DoD INFOCON levels.

Chairman Joint Chiefs of Staff Memorandum CM-510-99, *Information Operations Condition*, includes a table[18] identifying INFOCON levels, provides criteria for use in designating a specific level using indications and warnings about general threat information, and details recommended actions or countermeasures that can be taken during an attack. These actions must be carried out concurrently in all AORs for an effective defense. The approved DoD INFOCON levels reflect a defensive posture based on the risk 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). The criteria noted in the table includes identification of significant network probes, scans or network penetrations that result in denial of service of GIG resources, as well as a number of other activities. Examples of countermeasures include the development of redundancy of all mission-critical information systems (including applications and databases), the maintenance of a current prioritized list of their operational importance, the implementation of an increased level of auditing, the encouragement of a heightened awareness of all information system users, and the establishment of a method to reroute mission-critical communications through unaffected systems. Using indications and warning data and intelligence assessments to establish INFOCON levels, staffs are better able to advise

their commanders on recommended countermeasures for contingency and crisis action planning in the determination of courses of action and availability of infrastructure assets that are determined to be critical within the AOR. (For example, commands may be dependent on local communications or transportation services from the private sector.)

COMPUTER NETWORK DEFENSE SERVICE CERTIFICATION

The DoD has established policies to monitor and detect any type of disruption of service (e.g., denial of service attacks or computer viruses) that pose a threat to DoD information systems or computer networks. The DPO-MA can use existing CND policy and results collected by the CND Service Providers to monitor critical systems (e.g., GIG applications) and to assist Combatant Commanders in the identification of critical assets that support their contingency or crisis action planning. Additionally, the CNDS Certification Authority (CNDS/CA) can provide vulnerability information obtained during the certification process and through daily CERT operations by sharing data with the MASC and the JTF-GNO to help assess the readiness levels of the GIG.

The process of certifying the CNDS Provider includes the sharing of CND vulnerability information with the Combatant Commands, Services, and Defense Agencies. This process is an elaborate reporting hierarchy that ties these organizations together. The organizations in the hierarchy are designed to report any type of activity that appears to be malicious in nature – for instance, activity that could cause a denial of service or system disruption to the GIG.

Even though the JTF-GNO and the DoD CERT monitor disruptions to the GIG for potential computer network attacks, the data collected is not used for analysis to determine any impacts that attacks may have on the Defense Critical Infrastructure. The CND community needs to adopt an approach like that currently used by the DPO-MA for managing risk in its efforts to identify and defend against attacks to the Defense Critical Infrastructure.

NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (NS/EP)

Even though NS/EP in this context is not the responsibility of geographic and functional Combatant Commanders (with the exception of United States Northern Command [USNORTHCOM]), the NCS works very closely with industry partners in the telecommunications field to ensure that these services are available. Both the federal government (to include the DoD) and the private sector are dependent on these services to perform their missions and day-to-day business functions. President Reagan created the National Security

Telecommunications Advisory Committee (NSTAC) in 1982 for the purpose of providing "industry-based advice and expertise to the President on issues and problems relating to implementing NS/EP communications policy."[19] The committee has since "addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns."[20]

Combatant Commanders and Defense Agencies rely very heavily on the commercial sector to provide telecommunications services overseen by NSTAC members. The NCS incorporates a National Coordinating Center (NCC) for Telecommunications, which "leverages its unique joint government/industry structure and all-hazard emergency response capabilities to coordinate the initiation, restoration of United States government national security and emergency preparedness telecommunications services both nationally and internationally."[21] Yet, greater international cooperation is needed for the management of critical telecommunications and cyber assets and the maintenance of services during times of crisis. The DPO-MA should ensure that the NCC (as well as the MASC, as previously stated) is part of the Global NetOps C2 process, and that authority is provided to share information with organizations that control foreign communications resources. Knowing the reliability of both national and international telecommunications capabilities is a necessity for Combatant Commanders, particularly when they must communicate with national assets during times of crisis, as well as when commercial networks support command centers in foreign countries.

ESTABLISH ASSESSMENT PROGRAM FOR COMBATANT COMMANDERS

There are a number of assessment programs available for use in determining the readiness of commands. For example, the U.S. Army has used Unit Status Reporting (USR) results to measure the readiness of personnel and logistics. In *Title 10, United States Code*, Congress charged the Chairman of the Joint Chiefs of Staff (CJCS) with strategic planning responsibilities. The Chairman and the Combatant Commanders use the Joint Strategic Planning System (JSPS) as "the primary means employed to ensure that the force development activities of the Services and the operational planning conducted"[22] by the command authorities per national security policies are in accordance with CJCS direction to determine readiness. Additionally, the Chairman's Readiness System and the Joint Strategic Capabilities Plan (JSCP) can assist the Combatant Commander and Defense Agencies in determining the readiness of their commands. Many of the existing processes review traditional readiness; however, commanders should also examine domestic and foreign infrastructure assets as part of the risk

management equation. Even with established policies and procedures used by the Joint Staff, current assessment programs do not examine the defense infrastructure, to include the GIG. The systems used by the CJCS should be redesigned to address critical infrastructure assets used in support of contingency and crisis action planning missions.

To ensure DoD policy complies with Defense Critical Infrastructure requirements, the Full Spectrum Integrated Vulnerability Assessment (FSIVA) Program can be used to evaluate the accuracy of infrastructure data and provide Combatant Commanders and Defense Agencies with access to assessment information on vulnerabilities that could potentially impact their ability to conduct successful operations. FSIVAs include data on critical assets belonging to DoD and the U.S. commercial/private sector. They will also need to include the critical assets of foreign commercial/private sector and host nations that support joint and coalition missions. Additionally, the Component CERTs maintain a database of cyber vulnerabilities. The U.S. has established working relationships with organizations from a number of foreign countries that perform CERT functions -- relationships that could be useful in regard to a FSIVA Vulnerability Tracking Process. This process, which includes a draft concept for tracking the assessments, results, countermeasure recommendations and associated costs, remediation efforts, and follow-on assessments, is currently under development. The component CERTs currently use a similar tracking process to track cyber vulnerabilities for the purpose of risk mitigation of DoD critical assets.

The DoD has a requirement to evaluate the vulnerabilities of DoD critical assets. The DPO-MA has developed a program to address FSIVA requirements, standards and protocols in the Anti-terrorism/Force Protection (AT/FP), Critical Infrastructure Protection and Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) capability arenas; however, the FSIVA program does not make use of the documentation developed on cyber vulnerabilities during CND Certification processes. DoD Directive 8530.1[23] promulgated at the direction of the Deputy Secretary of Defense, describes the CND Certification of Component CERTs. It requires:

The DoD Components to establish Component-level CND Services (e.g., CERT) to coordinate and direct Component-wide CND operations for all Component information systems and computer networks.

The establishment of CND Certification Authorities at the DISA and the National Security Agency (NSA). DISA and NSA are responsible for certifying the capabilities of Component CERTs and providing overall technical and analytical, as well as coordination of CERT activities.

DISA to serve as the overall systems integrator, ensuring CND systems work together and that DoD begins to design and build CND into its computer networks as they are developed, rather than adding it on after the fact.

NSA to serve as the CND research and technology Program Manager, and provide Attack Sensing and Warning support to USSTRATCOM and DoD Components through the National Incident Response Center.

The establishment of a Defense CND Law Enforcement and Counterintelligence (CI) Center, which brings together the Defense Criminal Investigative and CI organizations. This organization is to be integrated into the structure of the JTF-GNO to coordinate law enforcement and CI investigations support of CND.[24]

DoD Instruction 8530.2, *Support to Computer Network Defense*, states that "Critical Infrastructure Protection (CIP) is an overarching national policy (Presidential Decision Directive 63) which seeks to assure continuity and vitality in critical national infrastructures, including both physical and cyber-based systems, and their associated information and communications infrastructures."[25] Additionally, the implementation of DoD Computer Network Defense strategy relies on the use of Information Assurance policies and technologies, which is vital to the protection of our national and defense infrastructure.

The development of diagnostic systems to support homeland security challenges is currently a high priority. "Because no part of our infrastructure can be fully protected from terrorist attacks, an essential element in a reasonably protected infrastructure is a diagnostic system to determine what is damaged, the extent of the damage, and a means to divert usage to other parts of the infrastructure system."[26] These proposed diagnostic systems can also be used to monitor critical infrastructure components, whether they are used for defense or the civilian sector.

The goal should be a U.S. infrastructure that is over time increasingly better protected from terrorism while remaining compatible with a globally competitive American economy. There are redundancies in the procedures outlined for protecting the DoD critical infrastructure and protecting the U.S. infrastructure from terrorist attack. There are planning issues with protecting both types of infrastructures. Challenges such as funding, technology, and metrics must be addressed. The Combatant Commander can continue to use the JSPS and the Chairman's Readiness System to assess combat readiness, but diagnostic systems such as the

Global NetOps C2 must also be integrated into the process to provide a complete range of capabilities for a more effective DCIP plan.

DCIP STRATEGY

The strategy for Homeland Defense and Civil Support focuses on achieving the Defense Department's paramount goal: securing the United States boundaries from attack by external enemies, while recognizing the need for an innovative approach to military operations by the DoD. The DPO-MA is chartered by the ASD(HD) to assist in institutionalizing and formalizing DCIP strategy. In this vein, the DPO-MA is responsible for distribution of the ASD(HD) DCIP funds throughout the DoD. The DCIP strategy is concerned with three classes of infrastructure and assets:

DoD owned infrastructures and assets that support the National Military Strategy;

Non-DoD infrastructures and assets that support the National Military Strategy; and

Non-DoD infrastructure assets important to national security. [27]

The strategy of the DCIP's foundation is an effects-based, mission-focused framework that provides a comprehensive and integrated risk management process for understanding, assuring, and (when necessary) protecting essential defense infrastructures. This framework is being institutionalized in the DoD with the establishment of policies to integrate the framework into the Planning, Programming, Budgeting, and Execution System (PPBES) as well as the DoD acquisition process.

STRATEGY AND GOALS

The DCIP Integrated Risk Management Strategy for fiscal years 2006-2011 consists of five major elements that are depicted in Table 1. Each element addresses a function of management regarding risks to and the provision of mission assurance for the protection of DoD critical infrastructure. The goals and management initiatives do not address operationalization of the DCIP Program, nor do they suggest recommendations for the integration of IA and CND concepts or methods to provide the Combatant Commander current situational awareness in regard to the infrastructure supporting his or her mission.

Elements of Risk Management Strategy	Goals & Management Initiatives
1. Understand Risks	Goal 1. Identify Critical Assets and Dependencies, and the Impact of Their Degradation or Loss. Goal 2. Conduct Vulnerability and Risk Assessments
2. Implement the Protection Program	Goal 3. Act On Remediation And/or Mitigation Recommendations
3. Respond to Incidents	Goal 4. Effectively Support Incident Management
4. Provide Adequate Program Support	Goal 5. Ensure An Effective Critical Infrastructure Program Foundation
5. Enabling Management Initiatives	Goal 6. Institutionalize DoD Critical Infrastructure Policy and the Program Goal 7. Provide and Manage Adequate Program Resources Goal 8. Foster Department-Wide Collaboration

TABLE 1. RISK MANAGEMENT STRATEGY[28]

Certain unresolved policy issues represent risks to successful execution of the DCIP Integrated Risk Management Strategy (IRMS). These issues span topics such as metrics, information sharing, burden-sharing for fixing vulnerabilities, DoD-DHS coordination, approaches to program acceleration, and education and training.

The ASD(HD) will work inside DoD and with interagency partners to address unresolved policy and program issues in order to enable the successful implementation of the DCIP IRMS for fiscal years 2006-2011.[29] The final result of a continued lack of sustained investment in the DCIP will be the inability of military commanders and DoD policy-makers to effectively manage the impact of failing infrastructure assets. This inability can only degrade DoD's capability to mobilize and project its forces, and provide sustainment and civil assistance -- essentially limiting or eliminating capabilities and factors crucial to the mission.

DEVELOP NEW TECHNOLOGIES AND PROCEDURES

The strategy for implementing Homeland Defense requires advances in information and communications technology that are essential to operationalizing the DCIP Program, particularly in regard to the integration of systems and applications across the DoD. The DCIP strategy recognizes the need to develop, manage, and coordinate research and development (R&D) requirements and acquisition activities across the DoD. The development of an integrated and

coherent suite of operational capabilities that complements and leverages ongoing DoD R&D and at the national level addresses the critical infrastructure needs of the warfighter and DoD critical infrastructure stakeholders is imperative. The DoD will continue to review existing R&D programs and promote the development of new initiatives in government, academia, and the private sector to support the formulation of the DCIP R&D program. This program will complement national level efforts in the Department of Homeland Security and will be responsive to Combatant Commanders, Joint Staff, and military Services.

"DCIP R&D will pursue research and development of the capabilities, technologies, and advanced concepts required by the DoD to:

Quickly identify vulnerabilities and risks to missions

Provide streaming situational awareness of defense critical infrastructure to include associated threats and hazards

Monitor and report threats and hazards against vulnerabilities

Rapidly provide alternative course of action recommendations to limit damage or disruption

Quickly recover from mission disruption

Dynamically reallocate critical infrastructure capabilities and resources necessary to defend, prevent, and defeat the threats and hazards."[30]

"The key participants required to achieve this goal are: the Director of Defense Research and Engineering (DDR&E), DPO-MA, the National Geospatial-Intelligence Agency (NGA), the Service laboratories, Defense Advanced Research Projects Agency (DARPA), the Joint Staff, Combatant Commanders, the Defense Threat Reduction Agency (DTRA), and Department of Homeland Security/ Science and Technology (DHS/S&T)."[31]

R&D efforts to achieve these goals will require substantial levels of funding. Many of the aforementioned organizations, however, may have ongoing research projects relating to the current war on terrorism. The DoD DCIP may be able to benefit from technological capabilities already developed for these projects. Additionally, a concerted effort to gain support and cooperation from both public and private sources should be launched—especially since much of the Defense Critical Infrastructure is also the nation's critical infrastructure (e.g. transportation, communication, and utility and energy systems).

An emerging operational concept called Network Centric Warfare (NCW)[32] (illustrated in Figure 2) may also be used by system architects supporting DCIP. But continued investment in communications and sensor technology throughout all components of each of the Services will be needed to fully achieve the objectives of NCW. An explanation of Net-Centric Warfighting is provided in Joint Pub 6.0: *Doctrine for C4 Systems Support to Joint Operations*. This doctrine highlights the information flow between sensors, command and control, and shooters, and recommends three components: an information grid, a sensor grid, and an engagement grid.[33] The diagram in Figure 2 highlights this information flow and depicts the architecture described above. The DCIP Enterprise Architecture should build upon the concepts of the information flow described in Figure 2 and integrate these three components into the GIG. The DoD has already benefited from the information grid and command and control components with the development of the Global NetOps C2 process. The next step for the DPO-MA is to explore new opportunities to utilize the senor grid to assist in monitoring critical infrastructure assets to support the Combatant Commander.

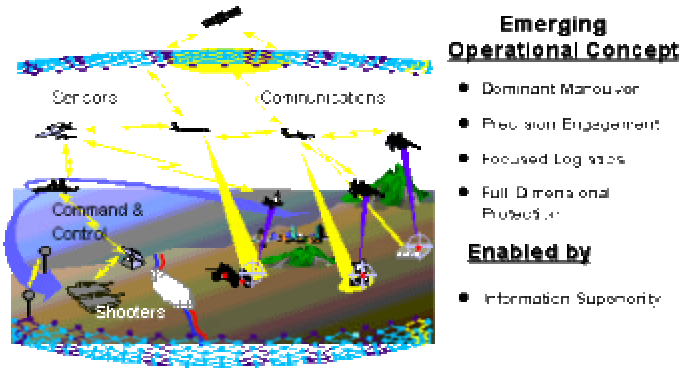

FIGURE 2: JOINT VISION 2020[34]

CONCLUSION

Effective operationalization of the DCIP Program and integrating the Defense-in-Depth strategy can provide the Combatant Commander with a new dimension to assess the command's ability to mobilize and fight. The maintenance of the elements of critical infrastructure that are essential to the mission of defense should be one of the highest priorities

of the U.S. Government, and certainly of the Combatant Commanders. The existing programs for the protection of Defense Critical Infrastructure must be reviewed and revised so that they provide a maximum of operational value and a minimum of confusion.

The final publication of DoD Directive 3020.ff is essential for the Office of the Assistant Secretary of Defense for Homeland Defense to have the authority to effectively establish and maintain the defense-related critical infrastructure on a global basis. However, there are a number of information assurance principles identified in this paper that should be incorporated in the new DoD directive. INFOCON levels must be understood throughout the DoD, not only by IA professionals but at all levels of Combatant Commands and Joint Task Forces. Leveraging the results from DCIP activities and using this information with the Global NetOps C2 process is critical to protecting the GIG, by ensuring all DCIP sectors participate in the information sharing process with the Combatant Commanders. Finally, FSIVAs can be used to measure the overall effectiveness of the DoD's Critical Infrastructure. The FSIVA process needs to continue to mature, particularly with respect to integrating IA policies and technology and ensuring that many of the tools used to conduct assessments are network enabled.

There are a number of benefits to operationalizing the DCIP Program at the Combatant Command level and in selected defense agencies. Providing the Combatant Commanders access to an entirely new set of integrated data that presents a common operational picture of the defense infrastructure, both government owned and commercially operated, is one of the most important benefits of operationalizing the DCIP Program. The DoD is also benefiting from the current effort to transform force structure and missions. The change in the global military posture is part of this transformation, which reflects a shift in military thinking. Transformation efforts must take into account the need for critical asset protection, whether this means the pre-positioning of equipment and supplies or the initiation of availability agreements with international partners. Transformation includes research on technologies that protect our critical infrastructure. For example, the Center for Strategic and International Studies (CSIS) has researched a number of new technologies in support of combating terrorism and protecting the United States critical infrastructure. This research has generated new sensor technologies and tools that can be used in command and control environments.[35]

There are a number of planning issues and funding requirements to operationalize the DCIP Program that are beyond the scope of this paper. Listed below, however, are some limited recommendations to be considered by the Critical Infrastructure Protection Integration Staff (CIPIS):

The DPO-MA should improve the FSIVA process by including the DIAP in their FSIVA working groups. ASD(HD) could leverage ASD(NII) practices in the DIAP to form policies that will implement FSIVAs as the metrics of DCIP.

The DPO-MA through the ASD(HD) should request support from the ASD(NII) to review comments on the CIP Vulnerability Assessment Capability Area CONOPs.

The DPO-MA should coordinate with the CND Certification Authorities to share assessment information.

The DPO-MA systems engineers need to ensure that the development of the Enterprise Architecture is integrated within the DoD CERT and JTF-GNO for release of Information Assurance Vulnerability Alerts and other approved countermeasures to protect the GIG, which is a DoD critical asset.

Include the results of the CND Certification of Component CERTs as part of the FSIVA process.

The DPO-MA should ensure that the NCC is part of the Global NetOps C2 process. Even though the NCC falls under the Department of Homeland Security, planners want to ensure information sharing continues with the DoD.

The Assistant Secretary of Defense for Network Information and Integration (ASD[NII]) has recognized potential threats and the fact that weaknesses in any portion of the Defense Department are of grave concern to the operational readiness of all components. The DoD is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information and the protection of its information infrastructure. The ASD(NII) needs to dedicate additional resources to help the ASD(HD) identify the strategic linkages between physical and cyber security. The integration of these two aspects of security into a single strategic approach will ensure DoD policies are consistent and resources are focused in support of the Combatant Commander.

WORD COUNT=5808

ENDNOTES

[1] The President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: U.S. Government, 13 October 1977), 22.

[2] A Department of Justice White Paper written on 22 May 1998 <http://www.usdoj.gov/criminal/ cybercrime/white_pr.htm>; Internet; accessed 14 February 2005, explains key elements of the Clinton Administration's policy on critical infrastructure protection. PDD 63 is the Clinton administration's policy on critical infrastructure protection. Clinton, William J., *Protecting America's Critical Infrastructure*, Presidential Decision Directive 63 (Washington, D.C.: The White House, 22 May 1998).

[3] This information is based on personal knowledge obtained by the author of this report from various sources over time.

[4] A copy of the Honorable Linton Wells testimony can be found in the following website <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17wells.html>; Internet; accessed 5 December 2004.

[5] The National Security Agency's Information Assurance implementation strategy <http://ax.losangeles.af.mil/se_revitalization/aa_functions/information_assurance/webpg/information_assurance.htm>; Internet; accessed 9 February 2005.

[6] Joint Chiefs of Staff, *Information Assurance (IA) and Computer Network Defense (CND)*, Chairman Joint Chiefs of Staff Instruction 6510.01D (Washington, D.C.: U.S. Joint Chiefs of Staff, 15 June 2004), GL-11.

[7] Department of Defense, *Defense Critical Infrastructure*, Defense of Directive 3020.ff (Washington, D.C.: U.S. Department of Defense, 10 May 2004), 2.

[8] "NetOps provides a common framework and command and control structure that will be used to conduct the global network operations mission in support of the USSTRATCOM Unified Command Plan 2002." Department of Defense, *Joint Concept of Operations for Global Information Grid NetOps* (Washington, D.C.: U.S. Department of Defense, 20 April 2004), 1.

[9] Ibid, 1.

[10] The MASC is a 24/7 operation located in Dahlgren, Virginia. Department of Defense, *Mission Assurance Support Center Standard Operating Procedures* (Dahlgren, VA: U.S. Department of Defense, March 2004).

[11] "The National Security Incident Response Center (NSIRC) provides near real-time reporting of cyber attack incidents, forensic cyber attack analysis, and threat reporting relevant to information systems." Statement by Mr. Daniel G. Wolf, Information Assurance Director, National Security Agency, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee for Technology and Procurement Policy, Joint Hearing on H.R. 3844: The Federal Information Security Reform Act of 2002, dated 2 May 2002, <http://www.nsa.gov/releases/relea00063.pdf>; Internet; accessed 9 February 2005.

[12] Department of Defense, *Joint Concept of Operations for Global Information Grid NetOps* (Washington, D.C.: U.S. Department of Defense, 20 April 2004), 24.

[13] Department of Defense, *Net-Centric Checklist* (Washington, D.C.: U.S. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004); <http://www.defenselink.mil/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.doc>; Internet; accessed 14 February 2004, 18.

[14] "The Defense Information Systems Agency created the Net-Centric Enterprise Services (NCES) program to provide enterprise services in support of the Global Information Grid. NCES will provide DoD organizations ubiquitous access to reliable, decision-quality information through a net-based services infrastructure and applications to bridge real-time and near-real-time communities of interest (COI). NCES will empower the edge user to pull information from any available source, with minimal latency, to support the mission. Its capabilities will allow GIG users to task, post, process, use, store, manage and protect information resources on demand for warriors, policy makers and support personnel." Department of Defense. DISA fact sheet describing NCES can be found at the following website <http://www.disa.mil/pao/fs/nces3.html>; Internet, accessed 15 January 2005.

[15] "A major initiative in DoD's communications transformation is Global Information Grid Bandwidth Expansion (GIG-BE), which will provide the robust network foundation to enable worldwide network-centric operations, supporting multiple transformation objectives. GIG-BE will create a ubiquitous "bandwidth-available" environment to improve national security intelligence, surveillance and reconnaissance, and command and control information-sharing. To implement GIG-BE, DISA is aggressively enhancing its current end-to-end information transport system, the Defense Information System Network (DISN), by significantly expanding bandwidth and physical diversity to selected locations worldwide. The program will provide increased bandwidth and diverse physical access to approximately 100 critical sites in the continental United States (CONUS) and in the Pacific and European theaters. These locations will be interconnected via an expanded GIG core. Specifically, GIG-BE will connect key intelligence, command, and operational locations with high bandwidth capability over physically diverse routes, and the vast majority of these locations will be connected by a state-of-the-art optical mesh network design." Department of Defense. DISA fact sheet describing GIG-BE can be found at the following website <http://www.disa.mil/main/prodsol/gig_be.html>; Internet; accessed 15 January 2005.

[16] "The genesis of the National Communications System NCS began in 1962 after the Cuban missile crisis when communications problems among the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state threatened to complicate the crisis further. After the crisis, President John F. Kennedy ordered an investigation of national security communications, and the National Security Council (NSC) formed an interdepartmental committee to examine the communications networks and institute changes. This interdepartmental committee recommended the formation of a single unified communications system to serve the President, Department of Defense, diplomatic and intelligence activities, and civilian leaders. Consequently, in order to provide better communications support to critical Government functions during emergencies, President Kennedy established the National Communications System by a Presidential Memorandum on

August 21, 1963. The NCS mandate included linking, improving, and extending the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability. On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472 which broadened the NCS' national security and emergency preparedness (NS/EP) capabilities and superseded President Kennedy's original 1963 memorandum. The NCS expanded from its original six members to an interagency group of 23 Federal departments and agencies, and began coordinating and planning NS/EP telecommunications to support crises and disasters." Background and history describing the National Communications System can be found at the following website <http://www.ncs.gov/about.html>; Internet; accessed 15 January 2005.

[17] "This memorandum establishes the Information Operations Condition for the DoD. INFOCON applies to the Joint Staff, Services, Combatant Commands, and Defense agencies, as well as joint, combined, and other DoD activities throughout the entire conflict spectrum – peacetime through war." Joint Chiefs of Staff, *Information Operations Condition*, Chairman Joint Chiefs of Staff Memorandum CM-510-99 (Washington, D.C.: U.S. Joint Chiefs of Staff, 10 March 1999), enclosure, 1.

[18] Joint Chiefs of Staff, *Information Operations Condition*, Chairman Joint Chiefs of Staff Memorandum CM-510-99 (Washington, D.C.: U.S. Joint Chiefs of Staff, 10 March 1999), enclosure, 4-5.

[19] Background about the National Communications System, <http://www.ncs.gov/about.html>; Internet; accessed 12 December 2004.

[20] Ibid.

[21] Mission statement for the National Coordination Center for Telecommunications, <http://www.ncs.gov/ncc/>; Internet, accessed 12 December 2004.

[22] Snyder, Gary W., Col, USAF. Joint Strategic Capabilities Plan, Lesson 3-5-L/S, Course 3 Curriculum, Joint Processes and Landpower Development (Carlisle, PA: U.S. Army War College, 28 October 2004), 22.

[23] "This directive requires all DoD information systems and computer networks to be monitored in accordance with 18 U.S.C. 2511 and DoD Directive 4640.6 in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security or function of DoD operations, DoD information systems or computer networks." Department of Defense. *Computer Network Defense*, Department of Defense Directive 8530.1 (Washington, D.C.: U.S. Department of Defense, 8 January 2001), 2.

[24] Ibid., 3-4.

[25] Department of Defense, *Support to Computer Network Defense*, Department of Defense Instruction O-8530.2 (Washington, D.C.: U.S. Department of Defense, 9 March 2001), 18.

[26] Kurt M. Campbell and Michele A. Flournoy, *To Prevail: An American Strategy for the Campaign Against Terrorism* (Washington, D.C.: Center for Strategic and International Studies, 2001), 254.

[27] Department of Defense, *Department of Defense Critical Infrastructure Program Integrated Risk Management Strategy, FY 2006-2011* (Washington, D.C.: U.S. Department of Defense, Office of the Assistant Secretary of Defense for Homeland Security, 7 April 2004), 1-2 .

[28] Ibid, 10.

[29] Department of Defense, *Department of Defense Critical Infrastructure Program Integrated Risk Management Strategy, FY 2006-2011* (Washington, D.C.: U.S. Department of Defense, Office of the Assistant Secretary of Defense for Homeland Security, 7 April 2004), 27 .

[30] Ibid, 24-25.

[31] Ibid, ,25.

[32] John J. Garstka, Network-Centric Warfare Offers Warfighting Advantage, Signal, May 2003, 58.

[33] Department of Defense, *Joint Concept of Operations for Global Information Grid NetOps* (Washington, D.C.: U.S. Department of Defense, 20 April 2004), Appendix C, "Information Superiority and Future Joint Warfighting," C-1.

[34] Department of Defense, *Joint Concept of Operations for Global Information Grid NetOps* (Washington, D.C.: U.S. Department of Defense, 20 April 2004), 59.

[35] Kurt M. Campbell and Michelle A. Flournoy, *To Prevail: An American Strategy for the Campaign Against Terrorism* (Washington, D.C.: Center for Strategic and International Studies, 2001), 253.

BIBLIOGRAPHY

John J. Garstka. *Network-Centric Warfare Offers Warfighting Advantage:* Washington, D.C.: Signal Magazine, May 2003.

Campbell, Kurt M. and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism* . Washington, D.C.: Center for Strategic and International Studies, 2001.

Clinton, William J. *Protecting America's Critical Infrastructure*. Presidential Decision Directive 63. Washington, D.C.: The White House, 22 May 1998.

Snyder, Gary W., Col, USAF. Joint Strategic Capabilities Plan, Lesson 3-5-L/S, Course 3 Curriculum, Joint Processes and Landpower Development. Carlisle, PA: U.S. Army War College, 28 October 2004.

U.S. Department of Defense. *Defense Critical Infrastructure Protection Strategy*. Washington, D.C.: U.S. Department of Defense, January 2003.

_____. *Defense Critical Infrastructure*. Department of Defense Directive 3020.ff. Washington, D.C.: U.S. Department of Defense, 10 May 2004.

_____. *Computer Network Defense (CND)*. Department of Defense Directive 8530.1. Washington, D.C.: U.S. Department of Defense, 8 January 2001.

_____. *Support to Computer Network Defense (CND)*. Department of Defense Instruction O-8530.2. Washington, D.C.: U.S. Department of Defense, 9 March 2001.

_____. *Department of Defense Critical Infrastructure Program Integrated Risk Management Strategy, FY 2006-2011*. Washington, D.C.: U.S. Department of Defense, Office of the Assistant Secretary of Defense for Homeland Security, 7 April 2004.

_____. Global *Information Grid Bandwidth Expansion Program Fact Sheet*. n.d. Available from <http://www.disa.mil/main/prodsol/gig_be.html>. Internet. Accessed 15 January 2005.

_____. *Information Assurance*. Department of Defense Directive 8500.1. Washington, D.C: U.S. Department of Defense, 24 October 2002.

_____. *Joint Concept of Operations for Global Information Grid NetOps*. Washington, D.C.: U.S. Department of Defense, 20 April 2004.

_____, *Net-Centric Checklist*. Washington, D.C.: U.S. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004.

_____. *Net-Centric Enterprise Services (NCES) Program Fact Sheet*. n.d. Available from <http://www.disa.mil/pao/fs/nces3.html>. Internet. Accessed 15 January 2005.

U.S. Department of Homeland Security. *Background and History Describing the National Communications System*. n.d. Available from <http://www.ncs.gov/about.html>. Internet. Accessed 15 January 2005.

_____. *Mission Statement for the National Coordination Center for Telecommunications*. n.d. Available from <http://www.ncs.gov/ncc/>. Internet. Accessed 12 December 2004.

U.S. Department of Justice. *Protecting America's Critical Infrastructure*. 22 May 1998. Available from <http://www.usdoj.gov/criminal/ cybercrime/white_pr.htm>. Internet. Accessed 20 November 2004.

_____. *Defensive Information Operations Implementation*. Chairman Joint Chiefs of Staff Instruction 6510.01b. Washington, D.C.: U.S. Joint Chiefs of Staff, 27 August 1997.

_____. *Information Assurance (IA) and Computer Network Defense (CND)*. Chairman Joint Chiefs of Staff Instruction 6510.01D. Washington, D.C.: U.S. Joint Chiefs of Staff, 15 June 2004.

_____. *Information Operations Condition*. Chairman, Joint Chiefs of Staff Memorandum CM-510-99. Washington, D.C.: U.S. Joint Chiefs of Staff, 10 March 1999.

U.S. Navy. *Mission Assurance Support Center Standard Operating Procedures*. Dahlgren, VA.: Naval Surface Warfare Center Dahlgren Division, March 2004.

Wells, Linton. *Testimony on Computer Network Defense*. 8 January 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/ 107thcongress/01-05-17wells.html>. Internet. Accessed 5 December 2004.