

GAO

Report to the Chairman,
Committee on Armed Services,
House of Representatives

March 2001

INFORMATION SECURITY

Challenges to Improving DOD's Incident Response Capabilities





United States General Accounting Office
Washington, D.C. 20548

March 29, 2001

The Honorable Bob Stump
Chairman
Committee on Armed Services
House of Representatives

Dear Mr. Chairman:

The Department of Defense (DOD) depends on interconnected information systems and communications networks for critical combat and business operations. Many of these systems and networks are interconnected through the public telecommunications infrastructure, including the Internet, and they may be targeted by an increasing variety of cyber attacks. If successful, these attacks could result in the loss or corruption of critical data, damage to information systems, or disruption of military operations. To address such threats, DOD has established organizations, known as computer incident response capabilities, at various locations worldwide. These organizations engage in a range of activities associated with preventing, detecting, and responding to computer incidents.

At the request of the former Chairman of the Military Readiness Subcommittee, we reviewed DOD's implementation of computer incident response capabilities and identified challenges to improving these capabilities. Our work focused on DOD organizations responsible for central incident detection and response operations that support military functions, including the Joint Task Force-Computer Network Defense (JTF-CND), the DOD Computer Emergency Response Team (DOD CERT), and the Global Network Operations and Security Center, managed by the Defense Information Systems Agency (DISA). We also reviewed computer incident response capabilities at the Air Force, Army, Marine Corps, and Navy. Much of the effort of these organizations has been aimed at monitoring unclassified systems, which often use the Internet and other elements of the public telecommunications infrastructure.

Results in Brief

Over the past several years, DOD has taken a number of steps to build incident response capabilities and enhance computer defensive capabilities across the department. During the 1990s, incident response organizations were gradually established throughout DOD—and the rest of the federal government—and they continue to mature in their capabilities. DOD now has computer emergency response teams (CERT) and incident response capabilities within each of the military services as well as DISA and the Defense Logistics Agency.¹ The JTF-CND was established in December 1998 to coordinate and direct the full range of activities within the department associated with incident response, including (1) preventive activities, such as conducting security reviews and issuing vulnerability alerts, (2) detection activities, including monitoring automated intrusion detection systems, (3) investigative and diagnostic activities, and (4) event handling and response activities, which involve disseminating information and providing technical assistance to system administrators so they can appropriately respond to cyber attacks.

We identified six areas in which DOD faces challenges in improving its incident response capabilities:

- Departmentwide resource planning and prioritization activities are not yet adequately coordinated to ensure that consistent and appropriate capabilities are available wherever they are needed.
- Critical data from intrusion detection systems, sensors, and other devices used to monitor cyber events and attacks are not yet being fully integrated across the department so that potential intrusions can be better identified and tracked.
- No departmentwide process has been established to periodically and systematically review systems and networks for security weaknesses on a prioritized basis and to use data from these reviews to improve overall security and configuration management practices.
- Compliance by individual units with departmentwide vulnerability alerts has not been consistently and comprehensively reported, leaving DOD unable to effectively track system and network repairs related to these alerts.

¹CERTs are organizations dedicated to providing support to systems administrators and others directly involved in responding to computer incidents. The term “incident response capability” is generally used to refer to organizations addressing the broader range of prevention, detection, and response activities, which are discussed in more detail later in the report.

-
- As demonstrated during the “LOVEYOU” virus event, DOD’s system for coordinating component-level incident response actions—known as the Information Operations Condition (INFOCON) system—has not always been effective in ensuring that component-level actions are consistent and appropriate.
 - DOD has not yet developed departmentwide performance measures to assess incident response capabilities to better ensure mission readiness.

DOD officials are aware of these challenges, and the department has undertaken initiatives to address certain of them. Specifically, DOD is (1) drafting a departmentwide incident response plan for internal review, (2) developing databases to centrally track cyber incidents and establishing common terminology for reporting cyber attacks across the department, (3) identifying network security gaps and developing procedures for prioritizing systems for security reviews, and (4) considering refinements to its INFOCON system. While promising, these initiatives are not yet complete and do not fully address the six challenges we identified during our review. Accordingly, we are recommending that the Secretary of Defense take additional action to address each of these challenges, including finalizing a departmentwide incident response plan, expediting development of mechanisms for departmentwide incident data integration and analysis, systematically prioritizing and conducting vulnerability assessments of high risk systems, establishing procedures to ensure consistent and complete reporting of compliance with vulnerability alerts, refining INFOCON procedures, and establishing a performance-based management process for incident response activities. In commenting on a draft of this report, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence concurred with the report and our recommendations.

Background

According to DOD, the department relies on over 2.5 million unclassified computer systems, 10,000 local area networks, and hundreds of long-distance networks for mission-critical operations. These systems and networks run on multiple hardware and software platforms consisting of interconnected mainframes, systems, and network operating systems that often operate over public, commercial telecommunication lines.

Security over these systems and networks involves multiple DOD and private sector organizations and is a difficult undertaking because of the ever-increasing number of cyber threats and attacks occurring over the Internet. Daily, DOD identifies and records thousands of “cyber events,”² some of which are determined to be attacks against systems and networks. These attacks may be perpetrated by individuals inside or outside the organization, including hackers, foreign-sponsored entities, employees, former employees, and contractors or other service providers.

Although historically DOD focused most of its security efforts on protecting the confidentiality of classified and sensitive information, this focus evolved as unclassified DOD systems and networks became increasingly exposed to cyber threats and attacks because of their connections with the public telecommunications infrastructure. After the “Morris Worm” attack crippled about 10 percent of the computers connected to the Internet in 1988, DOD acted—through the Defense Advanced Research Projects Agency—to establish the CERT Coordination Center at Carnegie Mellon University to address computer security threats. In 1992, the Air Force established the first military CERT to help address computer security threats and attacks internally. In 1994, a hacker from the United Kingdom raised concerns by launching a series of attacks against critical DOD research systems, demonstrating a need for better cyber defenses. Following these events, the Navy and Army established CERTs in 1995 and 1996, respectively.

During the 1990s, incident response organizations were also gradually being established throughout other agencies of the federal government. In 1996, the Federal Computer Incident Response Capability (FedCIRC) was established to assist federal civilian agencies in their incident handling efforts. Like DOD, civilian agencies continue to evolve and mature in their incident response capabilities.

²A cyber event is an action directed at a computer or network that could lead to an unauthorized result, such as unauthorized access to computerized information or resources.

Even as greater attention has been paid to incident response, cyber threats and attacks continue to affect the operations of DOD and other federal systems and networks. Since 1998, a number of federal systems have been subjected to a series of recurring, “stealth-like” attacks, code-named Moonlight Maze, that federal incident response officials have attributed to foreign entities and are still investigating. More recently, the “ILOVEYOU” virus attack affected electronic mail and other systems worldwide.³

According to DOD officials, thousands of potential cyber attacks are launched against DOD systems and networks daily, though very few are successful in accessing computer and information resources. In 1999 and 2000, the Air Force, Army, and Navy recorded a combined total of 600 and 715 cyber attacks respectively, during which intruders attacked DOD systems and networks in a variety of ways. Table 1 summarizes the numbers of recent documented cyber attacks reported by the military services.

Table 1: Cyber Attacks Reported by the Air Force, Army, and Navy for 1999 and 2000

Organization	Cyber attacks reported	
	1999	2000
Air Force	71	29
Army	367	299
Navy	162	387
Total	600	715

DOD and other organizations rely on a range of incident response activities to safeguard their systems, networks, and information from attack. These activities involve the use of various computer security tools and techniques as well as the support of systems and technical specialists. Incident response activities can be grouped into four broad categories:

- *Preventive activities*—such as conducting security reviews of major systems and networks and disseminating vulnerability notifications—

³*Critical Infrastructure Protection: “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000) and *Information Security: “ILOVEYOU” Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000).

are used to identify and correct security vulnerabilities before they can be exploited.

- *Detection activities* rely on automated techniques, such as intrusion detection systems⁴ and the logging capabilities of firewalls,⁵ to systematically scan electronic messages and other data that traverse an organization's networks for signs of potential misuse.
- *Investigative and diagnostic activities* involve (1) technical specialists who research cyber events and develop countermeasures and (2) law enforcement personnel who investigate apparent attacks.
- *Event handling and response activities*—responding to actual events that could threaten an organization's systems and networks—involve technical and system specialists who review data generated by intrusion detection systems and determine what needs to be done. This includes providing appropriate internal and external officials with critical information on events under way and possible remedies for minimizing operational disruption.

Objectives, Scope, and Methodology

The objectives of our review were to (1) identify DOD's incident response capabilities and how these capabilities are being implemented and (2) identify challenges to improving these capabilities. To do this, we worked at the DOD organizations primarily responsible for incident response activities at the departmentwide level and within the four services. Specifically, we worked at the U.S. Space Command in Colorado Springs, Colorado; the Joint Task Force for Computer Network Defense (JTF-CND) in Arlington, Virginia; the Defense Information System Agency's DOD Computer Emergency Response Team (CERT) and Global Network Operations and Security Center in Arlington, Virginia; the Air Force's Information Warfare Center and CERT in San Antonio, Texas, and Communication and Information Center, Rosslyn, Virginia; the Army's Land Information Warfare Activity and CERT at Fort Belvoir, Virginia; the Marine Information Technology Operations Center in Quantico, Virginia; and the Navy's Fleet Information Warfare Center and Computer Incident Response Team in Norfolk, Virginia.

⁴Intrusion detection systems are systems that collect information from a variety of automated sources, analyze that data for unusual patterns of activity, and report unusual activities. These systems may be configured to automatically respond to inappropriate activity by blocking transmissions.

⁵Firewalls are systems or devices that filter access between a private network and the Internet based on predefined rules that permit or deny communications.

At these locations, we obtained and analyzed information on (1) policies, procedures, roles, and responsibilities for incident response, (2) intrusion detection and other incident response tools and databases, and (3) key oversight and incident reporting procedures. Technical reports and database description documents were obtained and reviewed. We also reviewed operations and strategic planning documents and reports on computer security events, incidents, and intrusions for January 1999 through December 2000. Finally, we met with senior DOD officials in the Office of the Secretary of Defense to discuss departmentwide information security programs, strategies, and plans.

Our work was performed in accordance with generally accepted government auditing standards from April 2000 through January 2001. We did not verify the effectiveness of DOD's incident response capabilities and did not evaluate incident response capabilities within DOD support agencies, such as DISA. We obtained written comments on a draft of this report from the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. These comments are reprinted in appendix I.

DOD Has Progressed in Implementing Incident Response Capabilities

DOD has taken important steps to highlight the threat to its networks and systems and to enhance its ability to respond to computer incidents. For example, in 1997, DOD conducted a military exercise known as Eligible Receiver that demonstrated that hostile forces could penetrate DOD systems and networks and further highlighted the need for an organization to manage the defense of its systems and networks. A series of computer attacks against DOD systems in early 1998 further highlighted the need for a single departmentwide focal point for incident response.

In December 1998, DOD established JTF-CND as the primary department-level agent to coordinate and direct internal activities aimed at preventing and detecting cyber attacks, containing damage, and restoring computer functionality. The services—Air Force, Army, Marine Corps, and Navy—were directed to provide JTF-CND with tactical support through their CERTs and other supporting components. The U.S. Space Command assumed operational control over JTF-CND in October 1999. JTF-CND serves as the departmentwide focal point for incident response activities.

In 1998, DOD also established the Defense-wide Information Assurance Program (DIAP) to promote integrated, comprehensive, and consistent information assurance activities across the department. "Information

assurance” refers to the range of information security activities and functions needed to protect and defend DOD’s information and systems. While JTF-CND coordinates and oversees incident response activities on a day-to-day operational basis, DIAP’s responsibilities include coordinating DOD plans and policies related to incident response.

DOD’s network of CERTs, JTF-CND, and other related organizations engage in a variety of preventive, detective, investigative, and response activities, as described in further detail below.

Preventive Activities

DOD’s preventive activities are aimed at stopping cyber attacks or minimizing the likelihood that they will be successful in penetrating systems or networks through exploiting known vulnerabilities. These activities have included (1) vulnerability assessments of the security of DOD systems and networks, (2) using technical experts to try to surreptitiously gain access to systems and networks, thus exposing security weaknesses before adversaries can exploit them, and (3) alerting systems administrators to identified vulnerabilities.

Conducting vulnerability assessments can help ensure that system and security software is properly installed and configured and that the proper configuration is maintained through any updates or other modifications. Upon request, the Air Force, Army, Navy, and National Security Agency conduct vulnerability assessments of DOD systems and networks using a variety of automated computer security assessment tools. These tools automatically check systems and networks for known security weaknesses and generate reports summarizing results. During 2000, the Air Force, Army, Navy, and National Security Agency completed over 150 assessments that identified hundreds of vulnerabilities for commands to address. Upon request, the services and the National Security Agency use groups of technical experts to play the role of hackers and attempt to penetrate DOD systems and networks by exploiting known security weaknesses in commonly used systems and software. These efforts help prepare military forces to defend against cyber attacks and are often conducted during military training exercises. In addition, DOD established a Joint Web Risk Assessment Cell (JWRAC), staffed by reservists, to continually review DOD web sites to identify sensitive information. According to DOD officials, during its first 6 months of operation, JWRAC reviewed about 10,000 Web pages and identified hundreds of discrepancies for corrective action.

Even with these preventive efforts, new types of security vulnerabilities are being identified almost daily, and hackers are continually developing automated tools to take advantage of them. To keep its systems and networks current with the best available protection, such as up-to-date software patches, DOD depends on DISA's Information Assurance Vulnerability Alert (IAVA) process, which distributes alerts, bulletins, and advisories on security vulnerabilities, as well as recommendations for repairing security weaknesses, to the military services and Defense agencies. Since the program began in 1998, 27 alerts on potentially severe vulnerabilities and about 46 bulletins and advisories on lower risk cyber threats and attacks have been distributed to the services and Defense agencies for corrective action. Through their CERTs, the Air Force, Army, Marines, and Navy also disseminate to component commands hundreds of technical notifications on vulnerabilities that may require corrective action.

Incident Detection

In the area of incident detection, DOD relies largely on automated capabilities to identify significant cyber events—including attacks against systems and networks—as quickly as possible. Computer security technologies (such as intrusion detection systems and firewalls located at key network nodes) identify, track, and, if warranted, block inappropriate electronic traffic. Automated systems and tools are also used to collect, analyze, and display data on cyber events and to help establish a baseline of network activity to better identify anomalies and patterns that may indicate ongoing or imminent cyber attacks.

Currently, DOD reports that about 445 host-based and 647 network-based intrusion detection systems are in operation to help safeguard its over 2.5 million unclassified host systems⁶ and the networks supporting them. Host-based intrusion detection systems monitor individual computers or other hardware devices and are used to automatically examine files, process accounting information, and monitor user activity. Network-based intrusion detection systems examine traffic or transmissions from host-based systems and other applications traversing key locations on the network. Nearly all of these safeguard systems are based on commercial products, except for the Air Force's 148 Automated Security Incident Measurement Systems and the Joint Intrusion Detection Systems managed by DISA. The Air Force is also developing the Common Intrusion Detection

⁶A host system is the primary or controlling computer in an interconnected system generally involving data communications or a local area network.

Director System to correlate data from its intrusion detection systems and other sources in near real time to better track network activity patterns and identify cyber attacks. The Army and Navy have similar initiatives under way to develop databases for correlating information from intrusion detection systems and other devices. In addition, the Defense Advanced Research Projects Agency is funding research to develop more sophisticated intrusion detection systems.

Investigative and Diagnostic Activities

Investigative and diagnostic activities involve the use of technical specialists to research cyber events and attacks, to develop appropriate technical countermeasures, and to coordinate information with law enforcement personnel responsible for investigating and prosecuting intruders. Several DOD organizations, including the National Security Agency and Air Force, have established teams to examine the software code used to execute viruses and other cyber attacks and to help identify technical countermeasures for stopping the attacks or preventing them from infiltrating systems and networks. The JTF-CND, Air Force, Army, Marines, and Navy also coordinate with law enforcement and counterintelligence agencies when investigating potential criminal activities associated with cyber incidents. In addition, JTF-CND is developing systems and procedures to better coordinate and exchange information with law enforcement and counterintelligence agencies.

Event Handling and Response Activities

Finally, event handling and response activities involve disseminating information and providing technical assistance to system administrators so they can appropriately respond to cyber attacks. JTF-CND has been designated DOD's focal point for sharing critical information on cyber attacks and other computer security issues with internal and external partners. The military services also rely on CERTs to provide information on cyber attacks and immediate technical assistance to system administrators in the event of computer attacks. CERTs have the capability to deploy personnel to affected locations if system administrators need help implementing corrective measures or containing damage and restoring systems and networks that may have been compromised. JTF-CND also has developed standard tactics, techniques, and procedures for responding to cyber incidents and sharing critical information on cyber threats and attacks. Further, it is developing standard policies for sharing information with external partners, such as the National Infrastructure Protection Center (at the Federal Bureau of Investigation) and the Federal Computer Incident Response Capability (at the General Services

Administration). JTF-CND is also developing procedures to exchange critical information with the intelligence community and other Defense agencies.

DOD Faces Challenges in Improving Incident Response

Although DOD has progressed in developing its incident response capabilities, it faces challenges in several areas, including departmentwide planning, data collection and integration, vulnerability assessment procedures, compliance reporting, component-level response coordination, and performance management. Addressing these challenges would help DOD improve its incident response capabilities and keep up with the dynamic and ever-changing nature of cyber attacks.

Resource Planning and Prioritization for Incident Response Are Not Consistent Departmentwide

Because the risk of cyber attack is shared by all DOD systems that are interconnected with each other and the public telecommunications infrastructure, it is important that incident response activities be well coordinated across the department. An attacker who successfully penetrates one DOD system is likely to use that system's interconnections to attack other DOD computers and networks. Even if an attacker is at first unsuccessful in penetrating a particular system or network because it is well protected, such a person can go on to attack other systems and networks that may have vulnerabilities that are more easily exploited. For these reasons it is important that incident response activities be coordinated departmentwide to ensure that consistent and appropriate capabilities are available wherever they are needed.

DOD incident response officials agreed that coordination was important and report that the department has begun coordinating activities of the military services as part of the Program, Planning, and Budgeting System process. However, DOD has not yet identified departmentwide priorities or funding requirements for incident response. Instead, each of the services annually determines its own incident response priorities and funding requirements; as a result, the resources committed to incident response vary substantially. For example, Air Force officials estimated that they would spend over \$43 million for their Information Warfare Center and Computer Emergency Response Team in fiscal year 2000, whereas Navy officials estimated that they would spend less than \$4 million on their corresponding activities. Given widely varying resource commitments and the lack of established departmentwide priorities, it is uncertain whether systems and networks are being consistently and appropriately protected from cyber attack across the department. According to DOD officials, it is

difficult to identify departmentwide priorities, because no agreement has yet been reached on the core functions and characteristics of incident response teams among the multiple services and Defense agencies that currently field such teams. According to DOD officials, an effort is now under way at the department level to define those core functions and characteristics.

Critical Intrusion Data Are Not Integrated and Tracked Departmentwide

Integrating critical data from heterogeneous systems throughout an organization is important for effective incident response because it helps to assess and address threats, attacks, and their impact on systems and networks.⁷ Sufficient information is needed to establish what events occurred and who or what caused them. As attacks become more sophisticated, obtaining this information can become more and more difficult, requiring more and better-integrated data. Attackers may go to great lengths to disguise their attacks by spreading them over long periods of time or going through many different network routes, so that it is harder for intrusion detection systems to notice that attacks are occurring. Because of the threat of these kinds of attacks, it is increasingly important to collect intrusion data from as many systems and sensors as possible.

Although it has begun to develop several tools for tracking different kinds of incident data from across the department, DOD has only recently begun to implement key systems for integrating useful data from various intrusion detection systems and other heterogeneous systems, sensors, and devices for analysis. JTF-CND has taken steps to integrate intrusion data by sponsoring development of a Joint CERT Database to consolidate information on documented cyber attacks that have been collected individually by the services. According to DOD officials, the Joint CERT Database first became operational in January 2001. Work is also under way to develop a joint threat database as well as a database of law enforcement-related information. However, neither of these tools is yet operational.

Integrating intrusion data from across the department is a significant challenge because many different systems are in use that collect different kinds of data. Each of the services has deployed different intrusion detection systems to track anomalous network activity, and databases

⁷*Generally Accepted Principles and Practices for Securing Information Technology Systems*, Publication 800-14, National Institute of Standards and Technology, Department of Commerce (September 1996).

designed to track different types of specific data elements have been developed to synthesize raw data for analysis. Further, key information, such as data on insider attacks, is not yet tracked departmentwide.

To help overcome this difficulty, JTF-CND also launched a project to establish common terminology for incident response to help standardize reporting of cyber incidents and attacks throughout the department. However, the task force has not yet been able to bridge significant differences among the military services regarding how to classify and report computer incidents. For example, the Air Force currently does not report “probes” to JTF-CND because it does not consider these events harmful until its systems or networks are actually under attack.⁸ Internally, the Air Force identifies thousands of probes of its systems and networks daily and told us that reporting this information to JTF-CND would provide little insight on cyber attacks. However, the Army and Navy do report probes to JTF-CND. Experts believe data on probes can be used to assess the likelihood of an attack in the future. This is because potential intruders typically use a series of probes to gather technical information about systems so that they can tailor an attack to exploit the vulnerabilities most likely to be associated with those systems. Thus a series of probes against a system or systems may indicate that a more concerted attack against the same systems is likely in the near future.

Vulnerability Assessments Are Not Prioritized Departmentwide

Although DOD has had procedures in place since 1986⁹ for the military services to conduct vulnerability assessments of systems and networks and collect information on security weaknesses, no process has been developed, either at the department level or within the services, for prioritizing the conduct of vulnerability assessments. Instead, vulnerability assessments are generally conducted only when requested by component commanders or service-level audit agencies. Service officials agreed that there was no departmentwide process to identify which systems or networks faced the greatest risks and therefore should be assigned the highest priority for vulnerability assessments.

⁸Probes are attempts from unauthorized users to gather key technical information about systems in possible preparation for an attack.

⁹Department of Defense Instruction 5215.2, *Computer Security Technical Vulnerability Reporting Program (CSTVRP)*, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (September 2, 1986).

Neither is there a mechanism to follow up on the results of these assessments to verify that security weaknesses have been corrected. Generally, the assessment teams do not verify that corrective action has been completed as recommended. The problem is compounded by the fact that, in some cases, component officials are not responsible for all the systems and network connections identified as having security vulnerabilities. No procedures are in place to ensure that the systems outside their responsibility are fixed.

Furthermore, the information about vulnerabilities collected during these assessments is provided only to the affected components and not shared among the military services and Defense agencies. There is no process for ensuring that the results of these assessments are applied consistently and comprehensively to other similar systems and networks across the department. As a result, systems with the same vulnerabilities operating at other locations may not be addressed and thus may remain vulnerable. The DOD Office of the Inspector General (OIG) reported similar issues in 1997 and recommended that more be done to establish departmentwide priorities for conducting computer security reviews.¹⁰

Compliance With Information Assurance Vulnerability Alerts Cannot Be Adequately Gauged

Compliance with Information Assurance Vulnerability Alerts (IAVA) and other published guidance is critical because most successful attacks exploit well-known vulnerabilities. In 1999, for example, DOD reported that over 94 percent of its 118 confirmed cyber intrusions could have been prevented because they involved system access vulnerabilities that could have been remedied if organizations had followed recommendations already published through IAVAs and other security guidance. According to DOD officials, some of these fixes may have been completed but later inadvertently undone when systems were subsequently modified or upgraded.

IAVAs are used to notify the military services and Defense agencies about significant computer security weaknesses that pose a potentially immediate threat and require corrective action. The services and Defense agencies are required to acknowledge receipt of the alerts and report on the status of compliance with recommended repairs within specified time

¹⁰*DOD Management of Information Assurance Efforts to Protect Automated Information Systems*, Department of Defense, Office of the Inspector General, Report Number PO-97-049 (September 25, 1997).

frames. Also, DISA uses the IAVA process to disseminate technical bulletins and advisories about lower risk vulnerabilities and recommend ways to repair systems and networks. The military services, Defense agencies, and components are responsible for following recommendations in these notifications as they deem necessary.

Although military components are required to report on the status of compliance with IAVAs, current status reports provide limited insight on the extent to which systems and networks are being repaired. The information provided by the military services is not complete and may not accurately reflect compliance across DOD. In December 2000, the OIG reported that the Marines and Navy were the only services providing required IAVA compliance information to DISA.¹¹ In addition, based on information provided by the JTF-CND, corrective remedies specified in alerts, technical bulletins, and advisories issued as part of the IAVA process may not always be followed. Without full compliance and accurate reporting, DOD officials do not know whether critical systems remain vulnerable to known methods of attack.

DOD officials are aware that the IAVA monitoring process as currently implemented is not adequate, and a draft revision to the existing IAVA policies and procedures is being developed. In December 2000, the U.S. Space Command hosted a conference to address compliance reporting problems and discuss possible ways to link IAVA compliance reporting with existing operational readiness reporting requirements. However, at the time of our review, no final action had been taken to improve the compliance reporting process.

DOD's INFOCON System Has Not Effectively Coordinated Component-Level Response Actions

Coordinating responses to cyber attacks with internal and external partners, as well as law enforcement agencies, is important because it helps organizations respond to cyber attacks more promptly and efficiently, thus deterring cyber crime. Recognizing the need for this coordination, the Joint Chiefs of Staff established the Information Operations Condition (INFOCON) system in March 1999 as a structured, coordinated approach to react to and defend against attacks on DOD systems and networks. The INFOCON system defines five levels of threat and establishes procedures for protecting systems and networks at each level. These procedures were

¹¹*DOD Compliance With the Information Assurance Vulnerability Alert Policy*, Office of the Inspector General, Department of Defense, Report Number D-2001-013 (December 1, 2000).

modeled after security requirements for bases, commands, and posts that require coordinated and heightened security when attacks are imminent or under way. The INFOCON system focuses on network-based protective measures and outlines countermeasures to unauthorized access, data browsing, and other suspicious activity, such as scanning and probing.

Although the INFOCON system is a useful approach to standardizing incident response throughout DOD, the established measures provide only general guidance about the kinds of incident response activities that might be appropriate at each INFOCON level. Most decisions about what countermeasures to apply and how to apply them are left in the hands of systems administrators and other officials at individual DOD facilities. Lacking detailed guidance, the decision to apply countermeasures can be difficult for these officials in part because the countermeasures themselves may affect system performance. Inexperienced personnel may overreact and implement drastic countermeasures, resulting in self-inflicted problems, such as degraded system performance or communication disruptions. More detailed INFOCON guidance could outline operational priorities and other risk factors for consideration at each level to encourage consistent departmentwide responses to computer incidents.

According to JTF-CND, the “ILOVEYOU” attack demonstrated problems in applying INFOCON procedures uniformly across the department and poor communications regarding the appropriate INFOCON level for responding to the cyber attack. Once the “ILOVEYOU” virus had emerged, it took DOD several hours to produce a departmentwide recommendation on the appropriate INFOCON level for responding to the attack. Individual commands independently chose a variety of different levels and responses. For example, some commands made few changes to their daily operational procedures, while others cut off all electronic mail communications and thus became isolated from outside contact regarding the status of the attack. The INFOCON system did not provide any specific guidance on the appropriate INFOCON level or procedures for responding to a virus attack.

DOD recently organized a conference to examine ways to improve the INFOCON system, and DOD officials told us that revisions to the INFOCON procedures had been drafted that provide additional detail. However, at the time of our review, the revised procedures had not yet been issued. Further, according to a JTF-CND official, the revised procedures do not discuss the full range of system administrator actions that may be needed to address threats at each INFOCON level. The procedures also do not help systems

administrators determine which systems are most in need of defensive actions to maintain support for critical operations.

Useful and Complete Performance Measures Have Not Yet Been Established

Establishing and monitoring performance measures for incident response is essential to assessing progress and determining whether security measures have effectively mitigated security risks. Leading organizations establish quantifiable performance measures to continually assess computer security program effectiveness and efficiency.¹²

DOD officials stated that some quantifiable measures have been established for incident response. For example, the Air Force, Army, Marines, and Navy identify the number and type of cyber incidents and attacks that occur annually and report this information to appropriate senior officials within DOD. In addition, the Deputy Secretary of Defense established a goal of sharing information on significant cyber incidents within 4 hours.¹³

Although progress has been made, DOD officials agreed that more could be done to improve incident response performance measures and goals. For example, DOD could track information on the time required to respond to cyber attacks and the costs associated with managing attacks. The Navy now collects some information on the staff hours used to manage cyber attacks, which could be helpful in establishing performance measures. This information also could be used to establish baselines for reporting and responding to various types of cyber attacks and could be linked to combat readiness and mission performance objectives.

Space Command and JTF-CND officials indicated that some work was under way to establish performance parameters for incident response and to support joint military training requirements. Further, DOD conducts hundreds of computer security reviews of systems and networks annually but does not assess results from these evaluations to establish goals for improving computer security across the department. Information from these reviews could be used to identify patterns or security weaknesses across the Department and to establish targets to reduce security

¹²*Executive Guide: Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

¹³*Tactics, Techniques, and Procedures*, JTF-CND (November 15, 1999).

weaknesses within high-risk areas or for mission-critical systems and applications.

Conclusions

DOD has established significant incident response capabilities at the military services and mechanisms for centrally coordinating information assurance activities and incident response capabilities through DIAP and JTF-CND, respectively. However, DOD faces challenges in improving the effectiveness of its incident response capabilities, including (1) coordinating resource planning and priorities for incident response across the department; (2) integrating critical data from heterogeneous systems, sensors, and other devices to better monitor cyber events and attacks; (3) establishing a departmentwide process to periodically and systematically review systems and networks on a priority basis for security weaknesses; (4) ensuring that components across the department consistently report compliance with vulnerability alerts; (5) improving the coordination of component-level incident response actions; and (6) developing departmentwide performance measures to assess incident response capabilities and thus better ensure mission readiness. Acting to address these challenges would help DOD better protect its systems and networks from cyber threats and attacks.

Recommendations for Executive Action

We recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and the U.S. Space Command to work through DIAP and JTF-CND to

- finalize a departmentwide incident response plan, including objectives, goals, priorities, and the resources needed to achieve those objectives;
- expedite the development and enhancement of a complete set of systems for integrating and analyzing useful data from intrusion detection systems and other systems used to monitor computer security weaknesses, including tracking data on insider attacks;
- standardize terminology for computer incidents to facilitate the integration of incident data across the department;
- establish a systematic, departmentwide process for prioritizing and conducting vulnerability assessments of high-risk systems and networks and capabilities needed to support mission-critical operations;
- evaluate and monitor results from vulnerability reviews to ensure that recommended repairs have been made and have been applied to all similar systems throughout DOD;

-
- establish procedures to ensure consistent and complete reporting on the status of repairs required in IAVAs across the department;
 - link IAVA compliance reporting requirements to mission-critical systems and operations to increase awareness of the value of complying with technical bulletins and advisories distributed as part of the IAVA process;
 - refine INFOCON procedures to clarify the kinds of actions that need to be taken at each INFOCON level, especially with regard to priority systems, such as mission-critical systems; and
 - establish a performance-based management process for incident response activities to ensure that departmentwide goals as well as combat requirements are achieved, including establishing goals for (1) reducing the prevalence of known security vulnerabilities in systems and networks that support mission-critical operations and (2) timeliness in responding to known types of cyber attacks.

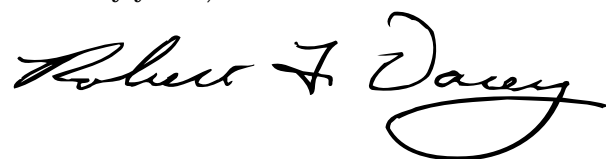
Agency Comments and Our Evaluation

In written comments on a draft of this report, which are reprinted in appendix I, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence stated that the department concurred with our draft report. In response to our second recommendation, DOD stated that the Joint CERT Database is now operational. We have clarified that this recommendation is to speed the development and enhancement of a complete set of systems for integrating and analyzing incident data, not just the Joint CERT Database. The department also provided technical comments that we have addressed as appropriate throughout the report.

We are sending copies of this report to Representative Ike Skelton, Ranking Minority Member, House Committee on Armed Services; to Representative Curt Weldon, Chairman, and Representative Solomon P. Ortiz, Ranking Minority Member, Subcommittee on Military Readiness, House Committee on Armed Services; and to other interested congressional committees. We are also sending copies to the Honorable Donald H. Rumsfeld, Secretary of Defense; the Honorable Paul Wolfowitz, Deputy Secretary of Defense; and the Honorable Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and Chief Information Officer. This letter will also be available on GAO's home page at <http://www.gao.gov>.

If you or your staff have any questions about this report, please call me on (202) 512-3317. Major contributors to this report included John de Ferrari, Karl Seifert, John Spence, and Yvonne Vigil.

Sincerely yours,

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, looping flourish at the end of the name.

Robert F. Dacey
Director, Information Security Issues

Comments From the Department of Defense



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

March 8, 2001

Mr. Joel C. Willemsen
Managing Director, Information
Technology Issues
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Willemsen:

This is the Department of Defense response to the General Accounting Office (GAO) draft report, "INFORMATION SECURITY: Challenges to Improving DoD's Incident Response Capabilities," dated February 1, 2001 (GAO Code 511706/OSD Case 3034). The Department concurs with the draft report.

The Department has made tremendous strides to improve our overall information assurance posture, but recognizes the need to strengthen our posture and implement our Defense-in-Depth Strategy. Your recommendations are very consistent with many of our ongoing efforts. The Department's comments to the recommendations are included at the Enclosure. Technical comments to the report have been provided separately.

My point of contact is Mr. Gary Guissanie, (703) 614-6132.

Sincerely,

Arthur L. Money

Enclosure



GAO DRAFT REPORT – DATED FEBRUARY 1, 2001
GAO CODE 511706/OSD CASE 3034

“INFORMATION SECURITY: CHALLENGES TO IMPROVING DOD’S
INCIDENT RESPONSE CAPABILITIES”

DEPARTMENT OF DEFENSE COMMENTS
TO THE REPORT & RECOMMENDATIONS

The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and the U.S. Space Command to work through the Defense-wide Information Assurance Program (DIAP) and Joint Task Force-Computer Network Defense (JTF-CND) to:

RECOMMENDATION 1: Finalize a department-wide incident response plan, including objectives, goals, and priorities and the resources needed to achieve those objectives. (p. 20/Draft Report)

DoD RESPONSE: Concur. A number of guidance documents for implementing DoD-wide Computer Network Defense (CND) have recently been published or are in final coordination, to include DOD Directives and Instructions on CND (8530.1), Information Assurance (IA) and CJCS Instruction and Manual 6510.01. These documents, particularly CND Directive 8530.1 and the follow-on Instruction, provide the necessary guidance for the development of coherent CND goals, objectives, and priorities. Several DoD led groups (e.g., Enterprise Sensor Grid & Information Assurance Architecture Working Groups, Network Operations Panel, etc.) are currently working to operationalize the guidance in these documents. The results of these working groups will directly impact incident response planning, goals, objectives, and resource requirements.

RECOMMENDATION 2: Expedite the development of the Joint Computer Emergency Response Team (CERT) database and other mechanisms for integrating and analyzing useful data from intrusion detection systems and other systems used to monitor computer security weaknesses, including tracking data on insider attacks. (p. 20/Draft Report)

DoD RESPONSE: The Joint CERT Database (JCD) is operational with all services feeding it. While work remains to refine the process, the database is in place and operating.

RECOMMENDATION 3: Standardize terminology for computer incidents to facilitate the integration of incident data across the department. (p. 20/Draft Report)

DoD RESPONSE: Concur. DOD Directives and Instructions on CND (8530.1), Information Assurance (IA) and CJCS Instruction and Manual 6510.01 are published or in final draft. While some work remains to refine definitions and taxonomy of computer incidents, we will standardize the terminology and update our directives.

RECOMMENDATION 4: Establish a systematic, department-wide process for prioritizing and conducting vulnerability assessments of high-risk systems and networks and capabilities needed to support mission critical operations. (p. 21/Draft Report)

DoD RESPONSE: Concur. As with the terminology with respect to computer incidents, there is a differing understanding among the Services with respect to “vulnerability assessments” and “Red Teaming.” We are writing a new directive to provide clearer policy in this arena, which should be completed by May 31, 2001.

RECOMMENDATION 5: Evaluate and monitor results from vulnerability reviews to ensure that recommended repairs have been made and have been applied to all similar systems throughout DoD. (p. 21/Draft Report)

DoD RESPONSE: Concur. The Department strives to make such efforts mandatory and uniform across all of our force structure and follow-up scans are conducted within a reasonable period of time. Continued oversight of this area is required.

RECOMMENDATION 6: Establish procedures to ensure consistent and complete reporting on the status of repairs required in Information Assurance Vulnerability Alerts (IAVA) across the department. (p. 21/Draft Report)

DoD RESPONSE: Concur. Same as item 5 response above. The requirement for consistent and complete reporting has been given increased emphasis by the Chairman, Joint Chiefs of Staff.

RECOMMENDATION 7: Link IAVA compliance reporting requirements to mission-critical systems and operations to increase awareness of the value of complying with technical bulletins and advisories distributed as part of the IAVA process. (p. 21/Draft Report)

DoD RESPONSE: Concur. IAVA compliance reporting requirements currently apply to all systems, with emphasis on critical systems.

RECOMMENDATION 8: Refine Information Operations Condition (INFOCON) procedures to clarify the kinds of actions that need to be taken at each INFOCON

level, especially with regard to priority systems, such as mission critical systems.
(p. 21/Draft Report)

DoD RESPONSE: Concur. Revised, more comprehensive, INFOCON procedures are currently being staffed. The draft was developed by USSPACECOM after their INFOCON conference in November 2000.

RECOMMENDATION 9: Establish a performance-based management process for incident response activities to ensure that department-wide goals as well as combat requirements are achieved, including establishing goals for (1) reducing the prevalence of known security vulnerabilities in systems and networks that support mission-critical operations and (2) timeliness in responding to known types of cyber attacks. (p.21/Draft Report)

DoD RESPONSE: Concur. This recommendation should be incorporated, and currently is to some degree, into the DoD Working Group on Information Assurance Metrics.

General Comment on Report: The comments on resource planning and prioritization for incident response capabilities, as noted in the first bullet on page 2, and the last paragraph on page 12, are overly broad. Resource planning and prioritization for incident response is coordinated department-wide as part of the Program Review process in the PPBS. However, it is not performed with the level of detail necessary to ensure consistent and appropriate capabilities are available, primarily due to the lack of metrics needed to make such judgements. This shortcoming has been addressed in the Computer Network Defense (CND) Policy that the Department has completed, and metrics are being developed to measure the adequacy of incident response capabilities, which will then be used in resource allocation.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

