GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284619

February 28, 2000

The Honorable Robert F. Bennett
Chairman
Special Committee on the Year 2000
Technology Problem
U.S. Senate

Subject: Computer Security: Reported Appropriations and Obligations for Four Major Initiatives

Dear Mr. Chairman:

This letter responds to your request for data on fiscal years 1998 through 2000 appropriations and obligations for four major computer security initiatives, including (1) the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC), (2) the Department of Defense's (DOD) Joint Task Force on Computer Network Defense (JTF-CND), (3) the General Services Administration's (GSA) Federal Computer Incident Response Capability (FedCIRC), and (4) GSA's Federal Intrusion Detection Network (FIDNet). We have also included data on amounts requested in the President's fiscal year 2001 budget, which was released February 7, 2000.

More than any other nation, the United States depends on interconnected computer systems—including the Internet—to support critical operations and services both in the public and private sectors. While beneficial, this reliance has increased the risks of computer-based fraud, inappropriate disclosure of sensitive data, and disruption of critical computer-supported operations and services. To better safeguard against computer disruptions within critical sectors of our economy, in January 2000, the President issued the National Plan for Information Systems Protection.[1] The National Plan calls for the government and the private sector to work together in a partnership to achieve computer security objectives. Each of the four initiatives covered by your request has a significant role in the President's recently released National Plan for Information Systems Protection.

As specified in the plan, (1) NIPC is to serve as the focal point for gathering information on threats to the critical infrastructures as well as facilitating and coordinating the government's response to such incidents, (2) JTF-CND is to monitor incidents and threats relating to national security and coordinate its assessments both within the Department of Defense and externally with appropriate agencies, counterintelligence organizations, law enforcement

[1] *Defending America's Cyberspace, The National Plan for Information Systems Protection: An Invitation to a Dialogue*, Version 1.0, White House, January 2000.

agencies, the private sector, and allies, (3) FedCIRC is to supplement these efforts by coordinating computer incident and response data and providing technical information, tools, and assistance, primarily to civilian agencies, and (4) FIDNet, through a network of intrusion detection devices, is to provide a centrally managed operational structure for processing and disseminating computer attack warnings to federal agencies.

Overall, officials told us that the programs we focused on are experiencing increased levels of activity and responsibility. As shown in table 1, the reported combined obligations and annual funding information reflects increases for the four programs between fiscal year 1998 and fiscal year 2001.

Table 1: Reported Annual Obligations and Requested Funding for Four Major Computer Security Initiatives (in millions)

	NIPC	USSPACECOM[a]/ JTF-CND	FedCIRC	FIDNet
FY 1998 obligations	$13.9	None	$4.7[b]	None
FY 1999 obligations	$16.1	$7.3	$2.2	None
FY 2000	$19.9[c]	$5.9[c]	$1.6[d]	$2.0[e]
Requested in President's FY 2001 budget	$20.4	$16.9	$15.4[f]	

[a]On October 1, 1999, the United States Space Command (USSPACECOM) was given responsibility for the computer network defense mission and JTF-CND operations.

[b]Figure provided to GSA by National Institute of Standards and Technology's (NIST) Comptroller includes combined obligations for fiscal years 1997 and 1998.

[c]Appropriated amounts reported for fiscal year 2000.

[d]Anticipated obligations reported for fiscal year 2000.

[e]Supplemental appropriation requested for fiscal year 2000.

[f]For fiscal year 2001, the President's budget includes a combined funding request for FedCIRC and FIDNet.

The information we obtained presents only a partial picture of the total funding because most of the programs are supported by related activities whose appropriations and obligations were not captured by our review. For example, JTF-CND relies on inputs and support from various Computer Emergency Response Teams (CERTs) funded by the military services and other components of the Department of Defense. In addition, data on the FBI's field office support for NIPC was not readily available and is not included in our summary.

Also, in order to obtain needed expertise, NIPC, JTF-CND, and FIDNet rely on staff detailees from other federal agencies or Defense components. The salaries for these individuals are not reflected in the summary figures obtained. We did not compile data on

appropriations and obligations for related activities or determine the salaries of detailees that were attributable to the programs we focused on because such information was not readily available and developing it was beyond the scope of this review.

Details on each of the four programs are provided in the enclosures to this letter. We developed the information presented in the enclosures based on discussions with officials at the agencies sponsoring these programs and on documents provided by their respective offices. We did not independently verify this information. We provided pertinent draft segments of this report to each of the agencies responsible for the four programs we reviewed. We adjusted the report, as appropriate, in response to their comments. We performed our work from December 1999 through February 2000 in accordance with generally accepted government auditing standards.

We are sending a copy of this response to the Honorable Christopher Dodd, Vice Chairman of the Special Committee of the Year 2000 Technology Problem; the Honorable William Cohen, Secretary of Defense; the Honorable David Barram, Administrator of General Services Administration; the Honorable Louis Freeh, Director of the Federal Bureau of Investigation; and the Honorable Jacob Lew, Director of the Office of Management and Budget. Please contact me at (202) 512-6257 if you or your staff have any questions. I can also be reached by e-mail at *mcclured.aimd@gao.gov* or contact Jean Boltz, Assistant Director, at (202) 512-5247 or by e-mail at *boltzj.aimd@gao.gov*.

Sincerely yours,

David L. McClure

David L. McClure
Associate Director, Governmentwide and Defense
Information Systems

Enclosures

Enclosure I

National Infrastructure Protection Center (NIPC)

Sponsoring Agency:

Federal Bureau of Investigation (FBI)

Date Initiated:

February 1998

Purpose and Program Description:

As called for in the National Plan for Information Systems Protection and as specified by Presidential Decision Directive 63, NIPC is to provide timely warnings of intentional threats, analyses, and law enforcement investigations and responses. Further, NIPC is intended to serve as the focal point for gathering information on computer network threats and investigations, as well as coordinating and sharing information among law enforcement agencies; national security organizations; and appropriate federal, state, and local agencies. To that end, NIPC produces various reports and products, including warnings, alerts, and advisories. According to the National Plan, NIPC is establishing a network of relationships with a broad spectrum of entities both within the federal government and in the private sector in order to promote awareness and provide training.

Funding:

According to FBI officials, the following information pertains only to obligations and funding for NIPC activities at FBI Headquarters. Additional obligations are attributable to FBI field office activities associated with NIPC. However, these amounts were not readily available, and additional work would be needed to compile them.

Obligations reported for fiscal year 1998	$13.9 million
Obligations reported for fiscal year 1999	$16.1 million
Appropriations reported for fiscal year 2000	$19.9 million
Amount requested in the President's fiscal year 2001 budget	$20.4 million

Enclosure II

Joint Task Force on Computer Network Defense (JTF-CND)

Sponsoring Agency:

Department of Defense (DOD)

Date Initiated:

December 1998

Purpose and Program Description:

In response to rising concerns identified by the President's Commission on Critical Infrastructure Protection and specified later in the National Plan for Information Systems Protection, DOD undertook several initiatives to improve computer security capabilities and manage and strengthen its information assurance activities. As part of this effort and while establishing a Defense-wide Information Assurance Program (DIAP), DOD recognized the need for a single organization to better manage and coordinate the defense of its computer network systems. Accordingly, DOD established the Joint Task Force on Computer Network Defense (JTF-CND) in December 1998 to

- provide indications and warnings of computer network attacks;
- coordinate and direct internal DOD actions to stop attacks, contain damage, and restore computer functionality;
- assess the effectiveness of computer network defensive actions and operational impacts; and
- coordinate with NIPC, DOD law enforcement agencies, DOD counterintelligence organizations, and other interagency partners regarding computer network attacks.

Under the Secretary of Defense, JTF-CND was established as an interim organization with the Defense Information Systems Agency (DISA) as a supporting agency. On October 1, 1999, the United States Space Command (USSPACECOM) was given responsibility for the computer network defense mission and JTF-CND operations. Space Command, however, will not assume complete funding responsibility for JTF-CND operations until October 1, 2000. The JTF-CND appropriations and obligations information we gathered does not reflect computer security support provided by other military components, such as monitoring and analysis done by the services (e.g., service-level computer emergency response centers). Space Command officials expect funding to increase significantly for fiscal years 2001 through 2005.

Funding:

The JTF-CND program was established in December 1998 (fiscal year 1999).

Obligations reported for fiscal year 1999	$7.3 million
Appropriations reported for fiscal year 2000	$5.9 million
Amount requested in the President's fiscal year 2001 budget	$16.9 million

Appropriations, obligations, and requested amounts represent the aggregate of information provided by DISA and USSPACECOM.

Enclosure III

Federal Computer Incident Response Capability (FedCIRC)

Sponsoring Agency:

General Services Administration (GSA)

Date Initiated:

- In 1996, by the National Institute of Standards and Technology (NIST)
- In October 1998, sponsorship transferred to GSA's Office of Information Security

Purpose and Program Description:

The National Plan for Information Systems Protection calls for the FedCIRC to provide the means for federal agencies to work together to handle computer security incidents, share related information, solve common security problems, and collaborate with NIPC and JTF-CND. According to GSA, FedCIRC currently

- provides technical information, tools, methods, assistance, and guidance to federal agencies;
- provides liaison activities and analytical support;
- supports collaborative relationships between federal civil agencies, DOD, academia, and private industry; and
- promotes awareness of computer incident response and handling procedures within the federal government.

In providing these services, FedCIRC obtains operational support from the Computer Emergency Response Team Coordination Center (CERT/CC) of Carnegie Mellon University's Software Engineering Institute. CERT/CC handles calls from federal agencies; provides reports, alerts and advisories to the FedCIRC; and provides computer security-related assistance to federal agencies. Also, FedCIRC is to coordinate with other federal agencies handling similar responsibilities—including NIPC and JTF-CND. GSA's plans call for management and funding for FedCIRC and FIDNet to be merged beginning in fiscal year 2001. FIDNet is discussed in enclosure IV.

Enclosure III

Funding:

Obligations reported for fiscal years 1997 and 1998	$4.7 million[a]
Obligations reported for fiscal year 1999	$2.2 million
Anticipated obligations reported for fiscal year 2000	$1.6 million
Amount requested in the President's fiscal year 2001 budget (FedCIRC and FIDNet combined)	$15.4 million

[a]Figures provided to GSA by NIST's Comptroller did not separate amounts for fiscal years 1997 and 1998.

Enclosure IV

Federal Intrusion Detection Network (FIDNet)

Sponsoring Agency:

General Services Administration (GSA)

Date Initiated:

Proposed in the President's January 2000 National Plan for Information Systems Protection.

Purpose and Program Description:

FIDNet was proposed to protect and defend selected civilian federal computer networks. The architecture of the proposed FIDNet focuses on connecting intrusion detection sensors at entry points to critical network segments. This proposed architecture will be based on existing Department of Defense and other security technology expertise.

According to the National Plan, the significant features of the proposed FIDNet include

- intrusion detection sensors at critical system nodes;
- automated incident reporting and handling; and
- a centrally managed operational structure for processing, disseminating, warning, and coordinating the status of the affected critical infrastructure systems.

The National Plan describes FIDNet as one of three programs—along with JTF-CND and the National Security Incident Response Center—that are to coordinate incident reporting and vulnerability assessments for key federal systems. According to a GSA official, FIDNet is still in the planning stages. GSA's plans call for management and funding for FedCIRC and FIDNet to be merged beginning in fiscal year 2001.

Funding:

The concept of FIDNet was proposed in early fiscal year 1999. On February 15, 2000, a White House press release announced that the President has requested a supplemental appropriation for fiscal year 2000 for several important cyber programs, including $2 million for the FIDNet Joint Program Office. According to a GSA official, the President's fiscal year 2001 budget requested combined funding for FedCIRC and FIDNet for $15.4 million.

(511680)

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested