Homeland Security

TecSec®, Incorporated has positioned itself as a central part of the solution set for the cross-agency sharing of information consistent with the charter of the Department of Homeland Security.

President Bush has said his objective in setting up the Homeland Security Department is to "minimize duplication, improve coordination, and combine functions that are currently fragmented and inefficient."

The legislation submitted calls for the department to secure critical infrastructures and to integrate relevant information, intelligence analysis and vulnerability assessments – all tasks that require sophisticated technology systems.

President Bush's legislation also calls for creation of an undersecretary for information analysis and infrastructure protection. A number of FBI agents from the National Infrastructure Protection Center (NIPC), which protects online commerce and the Internet against cyber attacks, would be moved into the new department. Several other agencies that deal with information analysis and infrastructure protection will be transferred to the department.

These agencies include:
- The Defense Department's National Communication System
- The Commerce Department's Critical Infrastructure Assurance Office
- The Computer Security Division of the National Institute of Standards and Technology
- The Energy Department's National Infrastructure Simulation and Analysis Center
- The General Services Administration's Federal Computer Incident Response Center

The new Department will rely on many technology systems, including communications, border security and information sharing as well as emergency preparedness and rapid response to biochemical and nuclear threats.

The new Department also will oversee the Domestic Emergency Support Team, the Strategic National Stockpile, the National Disaster Medical System and Nuclear Incident Response.

A key goal is improving the security of federal agencies, which have frequently been found to be lacking by the congressional watchdog agency, the U.S. General Accounting Office.

To that end, the Bush administration's proposed budget for next year (03) includes $5 Billion in new funding to improve security at federal agencies.

One technology effort, identified by the administration as one that *should command early focus*, is the development of interoperable identification control systems that would allow federal agencies to work with law enforcement as well as the private sector to correlate potential terrorist activity and threats.

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 1
Proprietary

July 15, 2002
TSWL012
All Rights Reserved

At least eight major agencies and numerous smaller ones will funnel information to the Homeland Security Department, which will serve as a "central clearinghouse to collect and analyze data related to terrorism" according to the Bush administration.

Today, "multiple intelligence agencies analyze their individual data, but no single government entity exists to conduct a comprehensive analysis of all incoming intelligence information and other key data regarding terrorism in the United States," the White House documents say.

That will be the job of the Homeland Security Department.

The new Department would be created from parts of existing agencies, absorbing the Coast Guard from the Transportation Department, the Immigration and Naturalization Service from the Justice Department, the Customs Service from the Treasury Department, the Federal Emergency Management Agency and smaller divisions from a number of other agencies.

The Homeland Security Department would inherit approximately 169,000 federal workers and a budget of $37.5 Billion.

Better intelligence sharing is a key element of the president's plan for the new Department. "Information must be fully shared so we can follow every lead to find the one that may prevent tragedy," Bush said in a televised address.

Information sharing has, however, been a technical and cultural problem for government agencies.

The new Department must also work with state and local first responders. Creating the connection and process for the necessary information sharing and distribution is a major priority, according to the House Government Reform Committee in its meeting on June 11th.

Rep. Jane Harman (D-Calif.) also said that any action taken by Congress likely would have to include a mandate for information sharing between federal and local responders because the administration's proposal does not include realigning the major sources for information – the FBI and the CIA.

Rep Mac Thornberry (R-Texas) co-sponsor of a House bill to create the Homeland Security Department has said, "A single structure will make it much easier to coordinate the exchange, whether it is investigative information coming into the new department or warning information being sent to the first responders".

A bill mandating that federal law enforcement and intelligence agencies share homeland security information with their state and local counterparts has the support of officials within the administration and was discussed in hearings on June 4th.

Following the hearing, the House Intelligence Subcommittee on Terrorism and Homeland Security passed the bill to the full House Judiciary committee.

The Homeland Security Information Sharing Act (H.R.4598) requires the administration to develop a plan within six months that will outline how sensitive but unclassified federal information can be shared with the appropriate officials within state and local law enforcement. The plan must also outline a process for redacting (removing) sensitive information from classified information so that it may be shared with state and local officials.

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 2
Proprietary

July 15, 2002
TSWL012
All Rights Reserved

The bill calls for the administration to outline information systems that can be used to share information in a timely manner. It fosters the use of existing systems such as the National Communications System and the National Law Enforcement Telecommunication System. It also directs the administration to apply the same model for redacting the classified information to other information sharing requirements, such as NATO and Interpol.

TecSec® is positioning itself with the National Communications System's Critical Infrastructure Protection program, the most established Information Sharing and Analysis Center in the Federal Government, as the preferred method to accomplish the required information sharing assignment.

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 22 Federal departments and agencies, and began coordinating and planning NS/EP telecommunications to support crises and disasters.

On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472 which broadened the NCS' NS/EP capabilities and superseded President Kennedy's original 1963 memorandum.

The NCS expanded from its original six members to an interagency group of 22 Federal departments and agencies, and began coordinating and planning NS/EP telecommunications to support crises and disasters.

With the United States Information Agency being absorbed into the U.S. State Department in October 2000, the NCS membership currently stands at 22 members.

Each NCS member organization is represented on the NCS through the Committee for National Security and Emergency Preparedness Communications (NS/EPC) --formerly known as the NCS Committee of Principals (COP) -- and its subordinate Council of Representatives (COR). The COP

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 3
Proprietary

July 15, 2002
TSWL012
All Rights Reserved

--formed as a result of Executive Order 12472, was renamed in October 2001 by Executive Order 13231: "Critical Infrastructure Protection in the Information Age."

The NS/EPC provides advice and recommendations to the NCS and the National Security Council through the President's Critical Infrastructure Protection Board on NS/EP telecommunications and its ties to other critical infrastructures. The NCS also participates in joint Industry-Government planning through its work with the President's National Security Telecommunications Advisory Committee (NSTAC), with the NCC's National Coordinating Center for Telecommunications (NCC) and the NCC's subordinate Information Sharing and Analysis Center (ISAC)[1].

The Office of the Manager, National Communications System (OMNCS) staff resources are organized into four divisions: Technology and Programs, Critical Infrastructure Protection (CIP) with the NCC, Plans and Resources, and Customer Service. The OMNCS is responsible for:

- Providing the expertise for the planning, implementing, administering, and maintenance of approved National Security and Emergency Preparedness (NS/EP) communications programs and NCS baseline activities.
- Conducting technical studies, analyses, and assessments pertaining to the effectiveness of NS/EP communications programs and the effects of these programs on the Nation's critical infrastructures.
- Consulting with the Committee for National Security and Emergency Preparedness Communications (NS/EPC), the NCS Council of Representatives (COR), and the President's National Security Telecommunications Advisory Committee (NSTAC) on issues pertaining to NS/EP telecommunications.
- Participating on Federal councils and boards, such as the President's Critical Infrastructure Protection Board and the National Infrastructure Advisory Council (NIAC), that develop telecommunications policies, standards, national initiatives, and performing research on emerging technologies.
- Monitoring international emergency telecommunications planning activities and offering assistance to international emergency planning groups.
- Developing, planning, and implementing National Communications System (NCS) strategic goals and objectives.
- Assisting individual NCS member organizations in developing efficient cost- effective solutions to complex communication/information requirements and resolutions to organizational communication/information issues[2].

The National Coordinating Center for Telecommunications (NCC) is a joint industry and Government staffed organization that assists in the initiation, coordination, restoration, and reconstitution of National Security and Emergency Preparedness (NS/EP) telecommunications services and facilities under crisis or emergency conditions.

Background: In 1982, the President's National Security Telecommunications Advisory Committee (NSTAC) recommended the government establish a mechanism by which the telecommunications industry and Federal Government representatives could coordinate initiation and restoration of NS/EP telecommunications services. In 1984, the NCC commenced

---

[1] National Communications System. Background and History. July 8, 2002
[2] National Communications System. Organizational Chart. July 8, 2002

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 4
Proprietary

July 15, 2002
TSWL012
All Rights Reserved

operations. Since that time, the NCC has responded to a full range of emergencies—from catastrophic hurricanes and other natural disasters to terrorist attacks and wartime activities.

The NCC is located at the National Communications System (NCS) Headquarters in Arlington, Virginia. Full-time telecommunications industry and Government representatives staff the NCC and serve as liaisons with their parent organizations.

The cooperation fostered between the telecommunications industry and the Government in the NCC has provided an operational focal point for all Government/ industry NS/EP telecommunications response across the spectrum of emergencies.

Highlights:

- During the recovery efforts following the terrorist's attacks of September 11, 2001, the NCC provided national and regional level support for response and recovery efforts to government and industry organizations and personnel. The NCC prioritized the communications assets, and restoration efforts, thereby ensuring NS/EP telecommunications needs and national priorities were met. A major goal was ensuring the successful opening and continued operation of the financial markets was achieved.
- In support of Presidential Decision Directive 63 (PDD-63), the NCS designated the NCC an Information Sharing and Analysis Center (ISAC) for the telecommunications sector. In June 1999, the NSTAC concurred with that designation. The ISAC achieved initial operating capability March 1, 2000.
- The NCC served as the collection point for network statuses for the telecommunications industry during the Year 2000 (Y2K) rollover. Over 80 companies nationally and internationally provided status updates into a Y2K database located in the NCC.
- The Telecommunications - Information Sharing and Analysis Center (Telecom - ISAC) is a function carried out by the National Coordinating Center for Telecommunications (NCC). The Telecom-ISAC mission is to facilitate voluntary collaboration and information sharing among Government and industry ISAC participants in support of Executive Order 12472 and the critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63). The Telecom-ISAC gathers and analyzes information on vulnerabilities, threats, intrusions, and anomalies of the telecommunications infrastructure to avert or mitigate impacts upon national security/emergency preparedness (NS/EP) telecommunications.

NCC MEMBERSHIP

(As of 02/07/2002)

INDUSTRY REPRESENTATIVES	FEDERAL PARTICIPANTS
AT&T	Department of State
Avici	Department of Defense
Bell South	Department of Justice
Boeing	Department of Commerce
Cisco Systems	Federal Emergency Management Agency (FEMA)

TecSec Incorporated
www.tecsec.com
Copyright 2010

Page 5
Proprietary

July 15, 2002
TSWL012
All Rights Reserved

INDUSTRY REPRESENTATIVES	FEDERAL PARTICIPANTS
Cincinnati Bell	General Services Administration (GSA)
Computer Science Corporation	Federal Communications
EDS	
ITT	
Lockheed Martin Commission	
Lucent	
Nortel Networks	
Qwest Communications	
Raytheon	
Science Applications International Corporation (SAIC)	
SBC Communications	
Sprint	
TRW	
U.S. Telecom Association	
Verizon Communications	
WorldCom	

Background: In accordance with PDD-63 and The National Plan for Information Systems Protection, the NCS established the Telecom-ISAC on March 1, 2000 in support of two goals outlined in the National Plan. The first is the establishment of the U.S. Government as a "model for information security," while the second is the development of a private-public partnership to defend the national telecommunications infrastructure. Although the concept of the ISAC was new, the NCS has been a central hub for sharing critical NS/EP telecommunications information among Government and industry in the NCC since 1984 and in the Network Security Information Exchange (NSIE) process since 1991.

The NCC -- established in 1984 based on a recommendation to the President by the National Security Telecommunications Advisory Committee (NSTAC) -- coordinates telecommunications restoration and provisioning during national disasters through Government/industry cooperation on a 24-hour basis. The NSIE process provides a forum for sharing information between Government and industry and among members of the telecommunications industry on threats to and vulnerabilities of the computer systems and databases controlling the Public Network.

Highlights:
- The Telecom-ISAC is currently the only ISAC with both Government and industry participants.

- The Telecom-ISAC builds on the history of cooperation and established trust relationships between the Government and telecommunications industry.
- Government representation: Departments of State, Defense and Commerce; the General Services Administration; the Federal Communications Commission; and the Federal Emergency Management Agency
- Full participation in the Telecom-ISAC is also open to companies that provide network services, equipment, or software to the communications and information sector, or Government NS/EP users. Additional participants are invited from competitive local exchange carriers (CLECs), Internet Service Providers (ISPs), vendors, software providers, federal, state, and local agencies.
- Telecom-ISAC operations are supported by senior information assurance analysts 24x7[3]. In the past months, TecSec has gathered the support of the Deputy Manager of the National Communications System, who characterized the TecSec solution as "the only offering that does not require the alteration of the existing infrastructure."

In addition, the Chief of the CIPP of the NCS, has instructed his staff to "get the TecSec solution in place."

In order to respond to these identified opportunities TecSec has aligned itself with teaming agreements with some of the major holders of existing contracts and the leading system integrators in the Federal Sector.

---

[3] National Communications System. www.ncs.gov. June 2002