National Security and Emergency Preparedness

Telecom News

2000, Issue 2

Published by the Office of the Manager, National Communications System, for the national security and emergency preparedness (NS/EP) community

# Lt Gen Raduege Becomes New NCS Manager

By Steve Barrett, Customer Service Division, OMNCS

Air Force Lieutenant General Harry D. Raduege, Jr., became the 14th Director of the Defense Information Systems Agency (DISA), and Manager of the National Communications System (NCS) during ceremonies held June 8 at Fort Myer, Virginia. He succeeds Army Lieutenant General David J. Kelley, who retired from the military during the same ceremony.

"Today, the flag has been passed to Lieutenant General Harry Raduege," said LTG Kelley in his farewell remarks on Fort Myer's Summerall Field. "He is the right guy at the right time. He's going to do a great job and I know that the teams at DISA and at the National Communications System are going to provide world class service as they've done for the past 3 years.

See Raduege Becomes New NCS Manager, page 4

**Air Force Lieutenant General Harry D. Raduege, Jr., accepts the colors of the Defense Information Systems Agency from General John M. Keane, the Army Vice Chief of Staff, during change of command ceremonies at Fort Myer, Virginia on June 8. In assuming command of DISA, Lt Gen Raduege also became Manager, National Communications System. (Photo by Robert Flores, DISA)**

## TABLE OF CONTENTS

*NS/EP Telecom News* is published quarterly under the auspices of Ms. Diann McCoy, Deputy Manager, National Communications System (NCS), to provide readers with analytical reports on issues relating to NS/EP telecommunications. Articles printed herein are for informational purposes only and do not necessarily represent official OMNCS or NSTAC positions. We invite NCS member organizations and other readers to comment on articles and suggest future topics for consideration.

For further information or additional copies, please contact:

Stephen Barrett
Office of the Manager
National Communications System

Customer Service Division
701 S. Court House Road,
Arlington, VA
22204-2198

PHONE: (703) 607-6211
FAX: (703) 607-4826

Home Page:
http://www.ncs.gov

# Defense Department, NCS, Honor LTG Kelley during Retirement Ceremony

By Steve Barrett, Customer Service Division, OMNCS

Army Lieutenant General David J. Kelley, the Director of the Defense Information Systems Agency (DISA) and Manager, National Communications System for the past 3 years, ended his 34-year military career June 8, at Fort Myer, Virginia.

In a ceremony hosted by General John M. Keane, the Army Vice Chief of Staff, and attended by Deputy Defense Secretary Rudy de Leon, LTG Kelley first relinquished command of DISA and the NCS to Air Force Lieutenant General Harry D. Raduege, Jr. He then retired before family, friends, West Point classmates, and members of the DISA/NCS community.

In recognition of his 34 years of military service, General Keane presented LTG Kelley with the Army Distinguished Service Medal. "In the past 5 years … the armed forces of the United States have achieved total and absolute information dominance," said GEN Keane. "We have the world's finest soldiers, sailors, Marines, airmen, and civilians operating the most technologically sophisticated systems in the world. You have played a major role in this development and the armed forces of the United States are better because of your service."

"Dave Kelley's life has been one devoted to country," said de Leon. "Through some of the most difficult years for our men and women in uniform, he believed that no matter the popular view, America would always need strong leaders to build a strong defense, and that is exactly the philosophy he brought to Washington."

De Leon said for the past 7 years—first as a member of the Joint Staff, then with DISA—LTG Kelley put his energy, optimism, and insight into anticipating what America's warfighters would need in the next fight. "He led the change to make sure our forces had the most advanced information they needed to fight and prevail," said de Leon.

In bidding farewell, LTG Kelley said he was "truly grateful" for the opportunity to serve the Nation and the chance to lead soldiers, sailors, airman, Marines, and civilians—all working together to harness information technology to benefit our warfighters. He praised his successor, saying that Lt Gen Raduege is "the right guy at the right time," and will do a great job.

He also gave credit to a list of past military leaders who provided LTG Kelley advice and guidance through his career—"great Americans all who understood … that our Nation's greatest resource is the young Americans who choose to serve our country."

Yet in saying goodbye,

**Colonel Thomas M. Jordan (left), Commander of the 3rd Infantry Regiment (The Old Guard) escorts Lieutenant General David J. Kelley in an inspection of troops during his retirement review held June 8 at Fort Myer, Virginia. LTG Kelley relinquished his duties as Director, Defense Information Systems Agency and Manager, National Communications System. (Photo by Robert Flores, DISA)**

LTG Kelley also expressed words of advice on telecommunications and readiness. “Being prepared in the command and control business means joint, interoperable information systems for today’s joint task force—as well as tomorrow’s—to ensure information superiority for our forces,” said LTG Kelley. He said that it was “wishful thinking” to believe that joint systems will just happen without hard work.

“The best technology in the world is useless if we can’t operationalize it in a way that helps the warfighter. We all have to work hard at jointness and internalize it as a key goal if we’re going to make it,” said LTG Kelley.

A native of Lafayette, Louisiana, LTG Kelley graduated from Lafayette High School in 1961. He earned a Bachelor of Science degree from the U.S. Military Academy, West Point, N.Y, in 1966 and a Master of Science degree in computer engineering from the University of Michigan in 1972.

His career spans command and staff assignments in Vietnam with the 1st Signal Brigade; Europe with the 8th Infantry Division; Fort Hood, Texas with the 1st Cavalry Division; and the Pentagon, where he served on the Army Staff and the Joint Staff.

LTG Kelley’s awards and decorations include the Defense Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit with Oak Leaf Cluster; the Bronze Star Medal with Oak Leaf Cluster; Meritorious Service Medal with three Oak Leaf Clusters; Army Commendation Medal; and Parachutist Badge and Ranger Tab.❖

## Raduege Becomes New NCS Manager, cont'd from page 1

I know, under your leadership Harry, the next Joint Task Force will be well served."

Nominated by Secretary of Defense William S. Cohen on April 6 to lead the NCS and DISA, Lt Gen Raduege comes to Washington from Peterson Air Force Base, Colorado. At Peterson, he served as Director of Command Control Systems, J-6, North American Aerospace Defense (NORAD)/ United States Space Command, and Director of Communications and Information, Air Force Space Command.

In welcoming the new Manager to Washington, Deputy Secretary of Defense Rudy de Leon said that in nearly 2 years at NORAD, Lt Gen Raduege "fused our space forces with our forces on Earth," mentioning the telecommunications successes with the U.S. forces in Kosovo. "In the coming years," said de Leon, "we'll look to you to ensure that all our forces can communicate and survive in the missions of the future."

After commenting on DISA's 40 years of service to DOD, Lt Gen Raduege addressed his eagerness to manage the NCS. "Since 1963, the National Communications System has worked in close proximity and relationship with DISA to nurture, promote, and achieve interagency cooperation and partnership between the Federal Government and the civilian telecommunications industry," he said. "For 37 years, the NCS has provided the necessary communications for the Federal Government under all conditions, ranging from a normal situation to national emergencies and international crisis, including nuclear attack."

The new Manager said he was honored to now lead and manage two organizations that have "…faithfully processed, encrypted, carried, displayed, and assured accurate information for our Nation's defense and emergency response." "I know that we face many challenges," said Lt Gen Raduege. "I can assure you, however, that [my wife] Julie and I, as a team, are ready. As in days past, the DISA [and NCS] team stands ready, and as always, our industry partners are ready. Together, we will answer the Defense Department's needs and our Nation's calling for the 21st century."

Lt Gen Raduege entered the Air Force in 1970 through the Air Force Reserve Officer Training Corps program at Capital University in Columbus, Ohio. He has spent his entire career in the areas of command, control, communications, and computers and space operations, serving in operations, maintenance, engineering, plans, budgeting, and readiness positions at every organizational level, from detachment through major command.

The Air Force selected him for the Air Staff Training Program and he served in the Directorate of Command, Control and Communications at Headquarters U.S. Air Force.

Prior to assuming his Peterson AFB position, Lt Gen Raduege was the Director of Command, Control, Communications and Computer Systems for U.S. Central Command. While there, he participated in a number of operations, including Southern Watch, Desert Focus, Desert Strike, Desert Thunder, Resolute Response, and ongoing maritime intercept operations in the Arabian Gulf.

He holds a Bachelor's degree in education from Capital University, Columbus, Ohio, and two Masters degrees—one in Business Management from Troy State University in Troy, Alabama, and a second in telecommunications from the University of Southern Mississippi.

Lt Gen Raduege is also a 1977 graduate of the Air Command and Staff College and a 1984 graduate of the Air Forces Staff College. He completed studies at the Air War College in 1989 and successfully completed the Executive Development Program at the National Defense University.

His military awards include Defense Superior Service Medal with Oak Leaf Cluster, the Legion of Merit, the Defense Meritorious Service Medal with Oak Leaf Cluster, the Meritorious Service Medal with five Oak Leaf Clusters, the Joint Service Commendation Medal, and the Air Force Achievement Medal. He also holds the Master Communications Badge, the Master Space Operations Badge, and Joint Chiefs of Staff Identification Badge.❖

# National Coordinating Center for Telecommunications (NCC) Adds Information Sharing and Analysis Center

The National Communications System's National Coordinating Center for Telecommunications (NCC) has established an Information Sharing and Analysis Center (ISAC) function as part of its national security/emergency preparedness (NS/EP) telecommunications mission.

The ISAC concept—a major objective of Presidential Decision Directive 63 (PDD-63)—will have the NCC gather, analyze, and disseminate private sector and Government information to participating telecommunications entities. The NCC becomes a central hub for sharing critical NS/EP telecommunications information on vulnerabilities, threats, intrusions, and anomalies among participating companies and between industry and the Government.

In announcing his National Plan for Information Systems Protection on January 7, President Clinton said the plan lays out two broad goals—"the establishment of the U.S. Government as a model for information security and the development of a public-private partnership to defend our national infrastructures." The President acknowledged the establishment of two ISACs at that time—the Telecommunications ISAC at the NCC, and the Banking and Finance ISAC.

Although the concept of the ISAC is new, the Government and the telecommunications industry have been sharing telecommunications information through the NCC for 16 years.

*As an ISAC the NCC will gather, analyze, and disseminate private sector and Government information to participating telecommunications entities.*

The NCC—founded based on a recommendation to the President from the National Security Telecommunications Advisory Committee (NSTAC)—was established in 1984 to coordinate telecommunications restoration and provisioning during national disasters through Government/industry cooperation on a 24-hour basis.

In June 1999, the NSTAC concluded that the NCC was already performing ISAC functions. Richard A. Clarke, the President's National Coordinator for Security, Infrastructure Protection and Counter-terrorism agreed with that conclusion.

Currently, the NCC has a variety of Government and telecommunications industry representatives—resident and non-resident—which monitor NS/EP telecommunications. Government members represent the Departments of State, Justice, Defense, and Commerce; the General Services Administration; the Federal Emergency Management Agency; and the Federal Communications Commission.

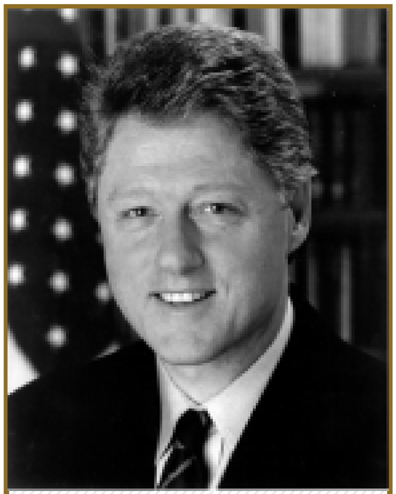
Industry representation in the initial telecommunications ISAC includes AT&T, Cisco Systems, COMSAT, Computer Sciences Corporation, EDS, ITT Industries, WorldCom, the National Telecommunications Alliance [representing the Regional Bell Operating Companies], Nortel Networks, Science Applications International Corporation, Sprint, the United States Telecom Association, and Verizon Communications.❖

# President Promoting Cyber Security for the 21st Century

By Steve Barrett, Customer Service Division, OMNCS

President Clinton launched the National Plan for Information Systems Protection on January 7, 2000, and announced new budget proposals for initiatives which would strengthen America's defenses against the emerging threats posed to our critical infrastructure, computer systems, and networks.

In a White House release, the President said the United States has benefited from the most advanced information technology (IT) infrastructure in the world. He added that this same IT infrastructure, however, makes us particularly vulnerable to cyber attack. "The most vital sectors of our economy—power generation, telecommunications, banking and finance, transportation and emergency services—are potentially susceptible to disruptions from hackers, terrorists, criminals or nation states."



**President Clinton launched the National Plan for Information Systems Protection on January 7, 2000. (White House photo)**

"We live in an age when one person sitting at one computer can come up with an idea, travel through cyberspace, and take humanity to new heights," said the President. "Yet, someone can sit at the same computer, hack into a computer system and potentially paralyze a company, a city or a government.

To help battle cyber threats, the President is promoting the establishment of Information Sharing and Analysis Centers (ISACs) for each of the critical infrastructures. In announcing the National Plan, the President identified two ISACs that are already operating—the banking and finance ISAC and the telecommunications ISAC. The telecommunications ISAC is operated by the National Communications System's National Coordinating Center for Telecommunications (NCC) and its private telecommunications industry partners.

The Clinton Administration plans to build on these partnerships to provide public education and cooperation with the private sector on a wide variety of information security issues. With the telecommunications and banking/finance industry ISACs already operating, the White House is working with the other sectors to help their proposed ISACs become operational in 2000.

The President said that thanks to the hard work of many people, U.S. computer systems were ready for Y2K. "But that experience did underscore how really interconnected we all are," said President Clinton. "Today, our critical systems—from power structures to air traffic control—are connected and run by computers. We must make those systems more secure so that America can be more secure."

The President has increased funding on critical infrastructure substantially over the past 3 years, including a 16 percent increase in the Fiscal Year 2001 budget proposal to $2.03 billion. He has also developed and funded new initiatives to defend the Nation's computer systems from cyber attack. To jumpstart the Fiscal Year 2001 program initiatives, the President will also propose a $9 million supplement this spring.

In the 18 months since the President signed Presidential Decision Directive 63 (PDD-63), the country has made significant progress in protecting our critical infrastructures. Last year, the President called for the development of a National Plan to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability. Version One, the "National Plan for Information Systems Protection: An Invitation to a

Dialogue," was released January 7.

White House sources said the first version of the plan "…invites a national dialogue leading to future editions." The plan lays out two broad goals: the establishment of the U.S. Government as a model of information security, and the development of a public-private partnership to defend our national infrastructures.

## Building the Public-Private Partnership

In addition to building partnerships with the private sector for critical infrastructure security, the President is committed to building other private sector relationships to protect our computer networks through the following initiatives:

***Institute for Information Infrastructure Protection.*** Building on a Science Advisory Panel, the White House is proposing to create an Information Infrastructure Institute which would combine federal and private sector energies to fill the gaps in critical infrastructure R&D that are not now being met in the private sector or the Department of Defense. It would also provide demonstration and development support in key areas like benchmarks and standards, and curriculum development. ($50 million)

***National Infrastructure Assurance Council.*** The President signed an Executive Order creating this advisory Council last year. Its members are now being recruited from senior ranks of the IT industry, key sectors of the corporate economy, and academia.

## The Federal Government as a Model of Information Security

The Clinton Administration has also developed and provided full or pilot funding for the following key initiatives designed to protect the Federal Government's computer systems:

***Working to Recruit, Train and Retain Federal IT Experts.*** The White House developed and provided FY 2001 funding for a Federal Cyber Services, Training and Education initiative, led by Office of Personnel Management (OPM) and National Science Foundation (NSF), which calls for two programs. The first is an ROTC-like program in which the Government pays for IT education (Bachelor of Science or Master of Science) in exchange for Federal service. The second is a program to establish competencies and certify our existing IT workforce. ($25 million)

Defending America's Cyberspace
National Plan for Information Systems Protection
THE WHITE HOUSE
WASHINGTON

**Richard A. Clarke, the President's National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, explains details of the President's National Plan for Information Systems Protection, along with then Commerce Secretary William Daley and White House Chief of Staff John Podesta. (White House photo)**

***Conducting Federal Agency Vulnerability Analyses and Developing Agency CIP Plans.*** Federal agencies have all developed CIP plans, and these have been reviewed by a newly created "Expert Review Team" (ERT) of Federal computer security experts. The White House has also established the ERT as a permanent team (at the Commerce Department's National Institute for Standards and Technology), with funding lines in FY 2000 and 2001. ($5 million)

***Designing a Federal Intrusion Detection Network (FIDNET).*** To protect vital systems in Federal civilian agencies, the Government is providing funding for development of a cyber "burglar alarm" which alerts the Federal Government to cyber attacks, provides recommended defenses, establishes information security readiness levels, and ensures the rapid implementation of system "patches" for known software defects. ($10 million)

***Piloting Public Key Infrastructure (PKI) Models.*** The Clinton Administration is funding seven PKI pilot programs in FY 2001 at different Federal agencies. ($7 million)

***Developing Federal R&D Efforts.*** In addition to the Institute for Information Infrastructure Protection, the

Clinton Administration has worked to ensure that research and development investments in computer security will grow more than 35 percent in the budget for FY 2001. ($621 million)❖

## Bennett Calls White House Plan "Important Step" Toward Comprehensive Information-Age Defense Policy

U.S. Senator Robert F. Bennett (R-Utah), Chairman of the Senate Special Committee on the Year 2000 Technology Problem, today called an Administration high-tech defense plan "an important first step" toward developing a national defense policy addressing cyber terrorism and information warfare attacks.

"This plan is a good first step toward defending the United States against 21st-century threats," said Bennett. "And it demonstrates that the Administration is serious about protecting Americans from Information-Age weapons and attacks."

The Senate Y2K Committee held a hearing and issued reports on information attacks during its two-year study of high-tech vulnerabilities in U.S. utilities, the health care industry, telecommunications, transportation, finance, Government, business and defense infrastructures.

An October report released by the committee found breaches of computer security increasing from 1,344 in 1993 to 4,398 in 1999. An FBI survey cited showed a 3-year increase in computer intrusions, with 30 percent of 521 respondents reporting cyber attacks.

In both the Fiscal Year (FY) 1996 and FY 1997 Defense Authorization Acts, Congress directed the President to create an architecture for defending against strategic information attacks, and Presidential Decision Directive 63 required that a plan be completed in 1998.

The Administration plan—released more than a year past the deadline—addresses the prevention and detection of cyber attacks; and the development of tools, techniques and expertise to assure national security in the Information Age.

"An effective national strategy would clarify responsibilities to different departments and agencies, create a high-tech attack warning system, and establish an efficient decision-making process integrating key Government and private industry sectors," said Bennett. "A successful plan would coordinate existing efforts of the high-tech, law-enforcement and defense communities to maximize effectiveness. Most importantly, it would ensure that infrastructure-protection would be factored into national policy decisions."

Bennett also said that a national plan must address international high-tech security concerns given the borderless nature of modern telecommunications, the Internet and e-commerce. Other lingering concerns involve the overlapping roles of the Defense Department, FBI and other agencies, which may encounter private-sector reluctance in sharing information about high-tech vulnerabilities.

*"This plan is a good first step toward defending the United States against 21st-century threats."*

"The President's plan is a good start," said Bennett. "But Congress and the Administration must work together to heighten an understanding about the nature of information attacks and their potential impact on the U.S. economy and national security. In addition, we must work in partnership with private industry to preserve privacy and competition while meeting modern defense challenges."❖

(Courtesy of the U.S. Senate)

# Senate Majority Leader Announces Working Group on Cyber Safety

Senate Majority Leader Trent Lott of Mississippi on March 27 announced the establishment of the Senate's Critical Infrastructure Protection (CIP) Working Group. The new CIP Working Group will serve as a central clearinghouse for information on cyber safety and critical infrastructure protection issues and efforts to address them.

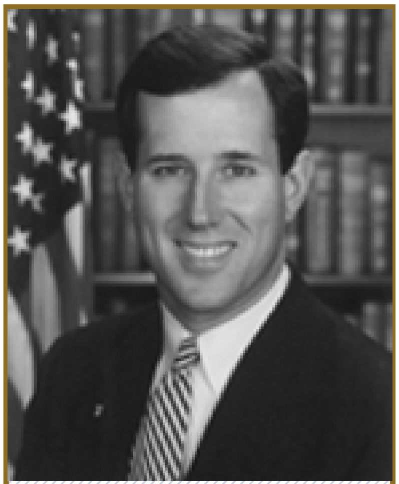
Senator Bob Bennett of Utah, chairman of the Senate Y2K Committee and of the Senate Republican High Tech Task Force, will chair the new working group. Senator Rick Santorum of Pennsylvania and Senator Spencer Abraham of Michigan will serve as co-chairmen of the group.

"High tech has brought advancement in education, communications, and the economy, but some real safety issues have emerged as well," Lott said. "Recent hacker attacks on major e-commerce and Government Web sites demonstrate the importance of information security to a well-functioning economy and a free society. This new working group will help provide communication that will lead to increased awareness and coordination."

Bennett said, "The interconnectivity and advanced capabilities of U.S. computer systems make the United States more vulnerable to cyber attacks than any other nation in the world. Such attacks could bring the U.S. economy to its knees. To prepare to meet this threat, CEOs [Chief Executive Officers] and CIOs [Chief Information Officers] must be made aware of its severity and have access to the most up-to-date, comprehensive information available.

"The CIP Working Group will serve as a central repository for this information and coordinate efforts to increase national awareness. The challenge of information warfare extends across organizational, industrial, and jurisdictional lines. To meet it, we must think horizontally."

Santorum said, "In this information economy where high tech is a driving force, the safety, privacy, and integrity of information is a top concern of all Americans. I look forward to working with my colleagues to facilitate discussions and new initiatives addressing cyber safety issues."



**Senator Rick Santorum**

*"The safety, privacy, and integrity of information is a top concern of all Americans."*

Abraham said, "Cyber security and on-line integrity are first among the many high tech issues that Government, industry and consumers must address to continue the success of our growing e-economy. This working group will be a valuable resource to keep everybody up-to-date and on the same page as we tackle these problems."

Other members of the working group include: Senate Committee Chairmen Phil Gramm of Texas, Banking; Orrin Hatch of Utah, Judiciary; Jesse Helms of North Carolina, Foreign Relations; John McCain of Arizona, Commerce; Frank Murkowski of Alaska, Energy; Richard Shelby of Alabama, Intelligence; Robert Smith of New Hampshire, Environment and Public Works; Ted Stevens of Alaska, Appropriations; Fred Thompson of Tennessee, Governmental Affairs; and John Warner of Virginia, Armed Services.

Other members are Senator Kay Bailey Hutchison of Texas, Senator Pat Roberts of Kansas and Senator Judd Gregg of New Hampshire.❖

(Courtesy of the U.S. Senate)

# President Holds Meeting on Ways to Make the Internet Safer

By Wendy S. Ross and Stephanie Cupp,
Washington File White House Correspondents

President Clinton met February 15 at the White House with executives of major e-commerce companies, computer security experts, reformed hackers, officials of civil liberties organizations and members of his Cabinet to discuss ways the U.S. Government and private industry can work together to make the Internet less vulnerable to hackers.

"The disruptions at several Web sites last week highlight how important the Internet has become to our whole way of life in America, and how vulnerabilities at one place on the Net can create risks for all," Clinton told those at the meeting.

In early February, hackers scrambled traffic and interrupted service to customers on several prominent e-commerce Web sites including Amazon.com, Yahoo and eBay. The Federal Bureau of Investigation (FBI) has launched a criminal investigation into the matter.

Clinton told the gathering that it is important that the Internet remain "open and free." But at the same time, he said, computer networks must be made "more secure and resilient, and we have to do more to protect privacy and civil liberties. And we're here to work together."

Peter Solvik, the Senior Vice President and Chief Information Officer of Cisco Systems, said "the events of last week show that everyone—Internet users, Internet companies, and Government—needs to work together to strengthen Internet security."

**Peter Solvik**
**Senior Vice President, CIO**
**Cisco Systems**

***"Everyone needs to work together to strengthen Internet security."***

He said the executives represented at the meeting have joined with leaders of other major Internet and information technology companies, as well as with officials of industry trade associations to work together on this issue.

"We're committed to increasing the security of the Internet by sharing information on cyber attacks, vulnerabilities, countermeasures, and best practices as a concrete way of improving security of the Internet," Solvik said. "We look to Government," he said, "to play an important role by coordinating this activity, ensuring its own systems are secure, and continuing to support important Research and Development (R&D) efforts."

Following the hour-long meeting, Clinton's Chief of Staff John Podesta said "many of the people in the room commented on the fact that many tools were out there to deal with security threats but many of the tools were not being used. We need to be more proactive."

Secondly, he said, the Federal Government must serve as a role model. Participants in the meeting, he said, supported Clinton's budget initiative of over $2 billion to invest in enhancing Internet security, increasing R&D and creating an institute to work in partnership with the private sector to do more research and development on the security issues.

And finally, he said, "there was a good deal of discussion that this is a global issue, a global network, a global problem. It can't be resolved simply by efforts of the United States Government, or even by the United States private sector. We need to work in partnership to enhance security, but we need to work around the world on solutions that, as the global information infrastructure is interconnected, will have a reach beyond our borders."

Commerce Secretary William Daley said, "Our information economy is strong, and it is resilient. But last week's incidents were really a wake-up call for all of us" to make sure that our systems are adequately protected.

Daley pointed out that the Department of Commerce has initiated a Partnership for Critical Infrastructure Security with the private sector. Officials of some 80 companies from different sectors of the economy met with Commerce Department officials in December to discuss these issues, he said, and met again February 22 "to try to develop mechanisms by which we can share information and move forward" in a multisector approach.

"It is not about the Government regulating this or taking steps to take actions that would at all impede the Internet because, of course, it is the dynamic engine that is driving our economy today, and we must keep that open," he said.

Harris Miller, President of the Information Technology Association of America, said the meeting with Clinton had been "very, very positive."

"We provided to the President and the other U.S. Government officials who were present, a statement, which has been endorsed by 38 companies just initially and 10 high-tech trade associations, committing to sharing information and working together through a mechanism, particularly to focus on cyberattacks, vulnerabilities, countermeasures, and best information security practices," Miller said. "Participation in this mechanism will be voluntary, industry-led, and maybe virtual."

"We also discussed with the President the important global nature of this challenge and the need to move forward in looking at this issue on a global basis," Miller said.

Maynard Webb, President of eBay Technologies, said that "There is no silver bullet for what we're going after. It's a difficult problem, but when we work together, we can solve it."❖

(The Washington File is a product of the Office of International Information Programs, U.S. Department of State.)

# New Viruses Exploit Wireless Vulnerabilities

By Ray Young, Technology and Programs Division, OMNCS

Last year, a cellular phone virus hoax spread through Lebanon. The focus of the hoax was a virus that infected the country's digital cellular network and the subscriber could receive the virus by answering a telephone call.

While this hoax needlessly spread panic among Lebanon's mobile subscribers, mobile devices may become a tool for virus writers to exploit. As mobile devices—such as cellular phones and Personal Digital Assistants (PDAs)—become smarter, they will increasingly become the targets of choice for virus writers and may be more vulnerable to virus attacks.

In the future, national security and emergency preparedness (NS/EP) capabilities may be impacted by attacks on these mobile devices. Many NS/EP functions are becoming more dependent on mobile and wireless communications and an adversary could potentially interfere with operations and target resources that are already limited. Attacks on mobile devices may become more common and force the National Communications System (NCS) and other Federal agencies to face a new threat that historically has not affected the public network.

There are some recent examples of attack attempts. On June 6, 2000, the Spanish telephone company Telefonica was the target of a malicious attack. A worm called Timofonica—similar in nature to the Love Bug virus—replicated itself among computer users. The e-mail message discredited Telefonica, and then asked the reader to click the attachment for more information. Once activated, the attached Visual Basic Script proceeded to damage the computer hard drive, then sent itself to all the listings in the user's address book.

An aspect of this Love Bug variation was that it contacted a short messaging system (SMS) gateway and dialed a random mobile subscriber's phone number. Through the SMS, the worm passed its message against Telefonica to the text display on the mobile handset.

Love Bug
Timofonica
Flood

*Anti-virus software companies are continuing their research efforts to protect cellular phones and PDAs.*

Fortunately, the worm did not infect cellular phones, nor did the phones pass any malicious code along. However, the attack demonstrated a vulnerability that exists with the new smarter mobile devices like cellular phones and PDAs.

An attack similar to Timofonica occurred in the United States last April. The National Infrastructure Protection Center released an advisory indicating that a virus spreading in the Houston, Texas, region was erasing hard drives and having the computer dial 911. This, in turn, was inundating the 911 system with bogus emergency calls that needed investigation.

During the Love Bug attack, the code would occasionally stumble across a fax machine or pager number in the Microsoft Outlook address book. While the code was unable to replicate itself or infect the device, the "code" would be printed out by the fax machine or displayed on the pager's screen.

Last March, WebTV users were hit by the Flood virus, which passes itself though e-mail, clogged the WebTV message boards and sent bogus e-mails to WebTV subscribers. This was surprising, because WebTV's set-top box network set-up and its use of HTML generally has left its subscribers immune to past viruses.

In the wake of the Timofonica worm and other serious attempts to attack wireless telecommunications, numerous anti-virus software companies are continuing their research efforts to protect cellular phones and PDAs. The NCS and other Federal Government agencies will pass information and updates on this subject to NS/EP telecommunications personnel and agencies as information becomes available.❖

# Technology Upgrades Help Keep TSP Vital to NS/EP Mission

By Betty Hoskin, Operations Division, OMNCS

Over the past few years, telecommunications services have become increasingly vital in coordinating and responding to national security and emergency preparedness (NS/EP) missions—both natural and manmade.

These events can inundate telecommunications service vendors with requests for repairs to existing services or orders for new services. The need to prioritize telecommunications services in this fast-changing world requires an ever-evolving program that will guide the telecommunications vendors of the Nation.

To help those telecommunications service vendors, the Office of the Manager, National Communications System (OMNCS), is constantly upgrading its Telecommunications Service Priority (TSP)

Program. Through the Office of Priority Telecommunications (OPT), the OMNCS manages the day-to-day operations of the TSP Program and serves as the point of contact for TSP matters.

After 10 years, both users and vendors feel that the TSP Program is a success, with State and local government organizations comprising the largest growth area for TSP restoration assignments in the last quarter of 1999. Contingency planning for the Year 2000 (Y2K) transition by State and local users accounted for much of the recent growth.

There are currently more than 29,000 NS/EP services nationwide protected by TSP authorization codes. The TSP codes ensure that telecommunications services critical to an organization's NS/EP mission will receive priority restoration from vendors before non-TSP services.

Today, the OPT is successfully applying information technology solutions to support its mission and enhance the administration and operation of the TSP Program. The OPT uses the Priority Telecommunications System (PTS) client/server platform to facilitate processing of administrative information while providing users, vendors and Federal sponsors with a flexible means of remotely accessing TSP information and on-line services.

**TSP Telecommunications Service Priority**

***After 10 years, both users and vendors feel that the TSP Program is a success.***

The client/server system is constantly being improved as advances are being made in the software packages used to develop the system. These enhancements include: custom designed reports for the PTS users; new search capabilities for the database; and easier system access and increased system security. In addition, the OPT uses the Internet for TSP outreach and information sharing.

In October 1999, the ability to submit TSP data electronically was introduced to the TSP Web site behind a secure sockets layer. The Web site application, E-Forms, is available to all TSP participants with an Internet browser 4.0 or better. They register to use the system and receive a logon ID and temporary password. This enables them to pass through the secure sockets layer and access the application. The submissions are saved behind the secure sockets layer. No data is passed across the Internet to protect the security of the data.

Electronic mail is used to notify the OPT and the E-Forms users that files are waiting to be picked up. These technologies and applications ensure that the TSP Program continues to serve the critical needs of NS/EP users into the 21st century.

Generally, NS/EP missions are assignments critical to maintaining readiness response for local, national or international events that could harm the population, damage property, or threaten the United States' NS/EP posture. The TSP Program grants common carrier telecommunications vendors the legal protection necessary to provide priority treatment to NS/EP services designated with TSP assignments over non-TSP services.

At the time of the AT&T divestiture, the Federal Communications Commission (FCC) realized that the United States needed a system to identify and prioritize critical NS/EP telecommunications services. This was also realized when the President's National Security Telecommunications Advisory Committee (NSTAC) acknowledged the need for a formal process to identify the Nation's critical NS/EP telecommunications services.

In addition, the NSTAC recognized the need to offer priority restoration and provisioning of telecommunications services when carriers become overwhelmed with service requests during crisis situations. As a result of an NSTAC recommendation, the FCC in 1988 issued the Telecommunications Service Priority Report and Order 88-341 establishing the TSP Program. This FCC Program founded the regulatory, administrative, and operational framework for priority provisioning and restoration of qualified NS/EP services.

The TSP Program is available to Federal and non-Federal organizations that have circuits/services that support NS/EP missions, including national security, public health and safety, and public welfare activities. Non-Federal TSP users must have a Federal agency sponsor for their TSP requests. The OPT can help the non-Federal user determine which Federal organization would be an appropriate sponsor, based on a shared mission.

Additionally, priority provisioning of telecommunications services has proven critical in supporting response to natural disasters, such as Hurricane Floyd and the Red River flooding, as well as defense activities such as the current military operations in Kosovo. These examples illustrate the importance of the TSP Program for critical infrastructure protection and as a vital link in the Nation's national security posture.

More information about protecting critical telecommunications services can be acquired in the following ways: visit the TSP Web site at http://tsp.ncs.gov; e-mail information requests to tsp@ncs.gov; mail requests to the Manager, National Communications System, Attn: OPT, 701 South Courthouse Road, Arlington, Virginia 22204-2198; or call (703) 607-4932.❖

# GETS Awareness Program Promotes Outreach Effort

By Zulfi Jamil, Technology and Programs Division, OMNCS

Fires, power failures, floods, and software problems are just a few incidents that can disable the telephone services of various regions throughout the United States. Besides natural and manmade disasters, congestion on the Public Switched Network (PSN), such as the well-documented "Mother's Day" phenomenon, can prevent emergency personnel from accessing telephone circuits.

In its efforts to provide emergency telecommunications over the PSN, the Office of the Manager, National Communications System (OMNCS), developed the Government Emergency Telecommunications Service (GETS). Emergency preparedness personnel can use GETS to complete emergency calls when they are unable to use regular telecommunications means.

In 1995, with focus from the Federal-level national security and emergency preparedness (NS/EP) community, the GETS user community was identified. Early in the GETS development stages, the OMNCS acknowledged that all disasters—whether natural, accidental, or intentional, begin as a local event. In recognizing this fact, the OMNCS identified the state and local emergency preparedness structure, consisting of emergency management agencies and first responders—law enforcement, fire and rescue departments, and emergency medical services—as candidate GETS users.

In 1996, the OMNCS began plans for a GETS awareness program. This effort would use an exhibition booth approach to distribute GETS information to emergency preparedness organizations at various conferences nationwide.

In an attempt to attend as many conferences as possible, the OMNCS staffs and maintains two booths to provide GETS information and demonstrate GETS capabilities to the NS/EP community. GETS personnel operating these booths distribute program brochures, videos, and supporting graphics. At the booths, names and addresses of interested conference participants are collected, and the OMNCS determines if the interested parties meet NS/EP requirements for GETS cards.

Today, the OMNCS deploys the GETS booth to over 100 conferences and exhibits across the United States. These deployments range from state, regional, and national conferences to Federal NS/EP-related exhibits. On average, the OMNCS deploys the GETS booth twice every month at a series of Federal and national conferences, including:

-National Emergency Management Association (NEMA)
-International Association of Emergency Managers (IAEM)
-National Disaster Medical System (NDMS)
-National Association of State Telecommunications Directors (NASTD)
-Association of Public Safety Communication Officers (APCO)
-National Sheriff's Association
-National Hurricane Conference
-Defense Department Emergency Preparedness Liaison Officers (EPLOs)
-National Guard Operations/Information Management Officers

In addition to these standard, recurring conferences, the OMNCS also participates in conferences sponsored by state emergency preparedness organizations and others, such as the American Red Cross and the Association of Contingency Planners, as staff are available.

The booth deployment drastically increases distribution of GETS cards to emergency response personnel. This outreach program also serves as an educational tool for the NS/EP professionals to further understand national emergency telecommunications programs. The outreach program opens up avenues for potential GETS users by allowing them to interact with GETS staff and other GETS card holders.

Based on these conferences, GETS staff members have made the following observations:

- Federal and non-governmental attendees often attend state and national conferences (and to a somewhat more limited extent, vice versa). Accordingly, the opportunity to provide GETS information to all levels of the NS/EP community is often present at the state conferences.

- Return visits are necessary to acquaint new members of the NS/EP community (at all levels) with GETS.

- Based on vulnerability to natural disasters, some states (such as Florida and California) should be visited annually whenever possible.

As of March 2, 2000, the OMNCS has issued over 42,000 GETS Personal Identification Number (PIN) cards to validated NS/EP users. This high volume of GETS cards is partially credited to the numerous nationwide deployments of the GETS booth.

For further information on GETS, its awareness and outreach program and the upcoming conferences at which the GETS booth will appear, visit the NCS home page at http:/www.ncs.gov.❖

# FCC Approves Bell Atlantic-GTE Merger with Conditions

The Federal Communications Commission (FCC) on June 16 approved applications to transfer control of FCC licenses and lines from GTE to Bell Atlantic, subject to enforceable merger conditions and spinning off substantially all of GTE's nationwide Internet business into a separate public corporation. The company formed as a result of the merger is called Verizon Communications.

The 25 merger conditions are designed to enhance local phone competition in the markets in which Bell Atlantic or GTE is the incumbent local exchange carrier (LEC), strengthen the merged company's incentives to enter local phone markets outside of its territories, and promote equitable and efficient advanced services.

[The merger of GTE and Bell Atlantic may eventually affect GTE's membership with the President's National Security Telecommunications Advisory Committee (NSTAC), and the National Coordinating Center for Telecommunications (NCC). Charles Lee, GTE's Chairman and Chief Executive Officer, currently represents GTE on the NSTAC and is a former chair. In addition, GTE is an active member of the NCC and its Information Sharing and Analysis Center (ISAC). Neither GTE nor Bell Atlantic has made any announcement in reference to their participation in NSTAC/NCC activities in the future.]

To ensure that the transaction does not violate the Telecommunications Act prohibition on providing long distance services without the necessary authorization, Bell Atlantic and GTE voluntarily proposed to spin-off GTE's Internet assets and offered a set of pro-competitive conditions.

### Internet Assets Spin-off

To comply with Section 271 of the Telecommunications Act, the merged company will transfer substantially all of GTE's Internet business into a separate public corporation to be known as Genuity (formerly GTE Internetworking). This section of the Act forbids a Bell Operating Company, such as Bell Atlantic, from providing long distance voice or data services to customers in its service territory before it demonstrates that its local phone market is open to competitors. To date, Bell Atlantic has only received authorization to offer long distance services in New York.

Under the ruling which was adopted, Bell Atlantic cannot convert its permissible 10 percent interest in Genuity into a greater equity ownership unless it receives long distance approvals covering 95 percent of its region where Genuity operates within 5 years.

Additionally, the merged company will not receive any economic benefit from the long distance services of Genuity for those states in which Bell Atlantic is restricted from providing long distance services. Specifically, the merged company will give to Genuity shareholders any gain in Genuity's value that is attributable to Genuity's operations in states during the period of time in which the combined company is restricted from offering long distance services. This provides a powerful incentive for Bell Atlantic to accelerate its efforts to open its local phone markets to competitors.

### Merger Conditions

The merger conditions are designed to accomplish the following five public interest goals:

1. Promote advanced services deployment;
2. Enhance the openness of the merged company's in-region local telecommunications markets;
3. Foster out-of-region local competition;
4. Improve residential phone service; and,
5. Provide for enforcement of the merger.

Absent the merger conditions, the merger would likely lead to the following public interest harms:

1. The merger would remove one of the most significant potential participants in local telecommunications mass markets within Bell Atlantic's existing territory.
2. The merger would reduce the ability of the FCC to implement the market-opening requirements of the 1996 Act through comparative practice oversight (benchmarking) methods.
3. The merger would increase the incentive and ability of the merged entity to discriminate against its rivals, particularly with respect to the provision of advanced telecommunications services.

### Wireless Issues

The FCC's order finds that the merger of the companies' wireless operations would be pro-competitive and grants the companies' applications to transfer control of GTE's wireless licenses to Bell Atlantic on the condition that they comply with the Commission's cellular cross-ownership and CMRS spectrum cap rules.

Absent divestiture, the merger of Bell Atlantic and GTE would create nearly 100 overlaps under these rules. A number of these overlaps will be resolved by the recently approved sale of properties to ALLTEL. The companies have informed the Commission that negotiations to sell the remaining properties are proceeding, and that additional filings are imminent.

Certain properties, however, will be placed in trust for purposes of divestiture to third parties, and applications to place properties in trust are on file with the FCC.

**International Issues**

The FCC's order also finds that the public interest will be served by transferring control of GTE's international section 214 authorizations to Bell Atlantic, subject to the condition that the merged company's subsidiaries be classified as dominant international carriers in their provision of service on the U.S.-Gibraltar, U.S.-Dominican Republic, and U.S.-Venezuela routes.

The action was taken by the Commission June 16, 2000, by Memorandum Opinion and Order (FCC 00-221). Chairman William Kennard, Commissioners Susan Ness and Gloria Tristani, with Commissioner Harold Furchtgott-Roth and Michael Powell concurred in part and dissented in part. Commissioners Ness, Furchtgott-Roth, Powell and Tristani issued statements on the action.❖

(Story courtesy of the Federal Communications Commission)

# Bates Replaces Fischer as GSA FTS Commissioner

The U.S. General Services Administration (GSA) announced on March 7 that Sandra Bates is the new commissioner of GSA's Federal Technology Service (FTS). Bates replaced Dennis Fischer, who retired April 2, 2000, after 30 years of Federal service.

Fischer had been the Commissioner and Bates Deputy Commissioner for the past 2.5 years. In announcing Bates' appointment, GSA Administrator David J. Barram said that Fischer—a member of the National Communications System's Committee of Principals—has been a terrific commissioner during some very challenging times. "He has brought us strategic leadership, a passion for connecting with our customers, and is a strong advocate for the Federal employee," Barram said.

"I have every confidence that FTS will continue to thrive under the leadership of the new commissioner, Sandra Bates. Her experience and knowledge of this fast moving world of technology and telecommunications," Barram said, "are precisely what we need to thrill our Federal customers. I wish them both the very best as they take this next step in their careers."

Bates began her Federal career with GSA in 1969, working on the original FTS program. In 1979, she moved to the National Aeronautics and Space Administration (NASA), starting as a telecommunications program manager, and was appointed chief of communications in 1993, with responsibility for all command and control programmatic networks. She received the NASA Exceptional Medal, and received Fed 100 honors in 1994, 1996 and 1999.

In 1996, Bates returned to GSA as Assistant Commissioner for Service Delivery for FTS. She became Deputy Commissioner in 1997 and was awarded the prestigious Presidential Rank Award of Meritorious Executive by President Clinton in 1999.

"It's been a real privilege to serve as Dennis Fischer's Deputy Commissioner, under the leadership of Dave Barram," Bates said. "An essential factor in the unprecedented business growth in FTS over the past two years has been Dennis' drive and vision. He has taught FTS employees the importance of strong customer relationships."

"He never forgets to remind us that our people are our most precious asset," said Bates. "These lessons form a legacy we can all be truly proud of. I can't think of a better place to be than stepping into the position of Commissioner behind Dennis. FTS, the industry and our customers are undergoing exciting changes, and I'm excited to be taking on this new role at this time."

Fischer, who will become a Department Head and Vice President in the Sales and Integrated Solutions Department of VISA, USA, based in McLean, Virginia, said in a message to all FTS employees that his greatest delight has come from “working with our only precious asset, all of you.”

He wrote, “I have had a wonderful career and this experience has been its highlight…my Federal Government career is ending…wishing all of you the best of success as you ‘thrill’ the customer, ‘grow’ the business and make FTS the ‘best place to work’ in the Federal Government.”

Sandra Bates

Dennis Fischer

**Sandra Bates assumed the post of Commissioner of the Federal Technology Service, following the retirement of Dennis Fischer on April 2, 2000. Fischer retired after 30 years of Federal service and was the General Services Administration member of the National Communications System Committee of Principals. (Bates photo courtesy of GSA, Fischer photo by John Kandrac, DISA)**

FTS provides telecommunications services and information technology solutions for its Federal customers. Each year, FTS provides more than $4.3 billion in products and services. It provides telecommunications such as global voice, data and video.

In other GSA appointments, Charles Self will become the FTS’ new deputy commissioner and Robert Suda, the current Chief Financial Officer and Acting Chief Information Officer, will replace Self as Assistant Commissioner of its Office of Information Technology Integration. Both appointments were effective April 2, 2000.

In making the announcement, Bates said, “Charles Self has served FTS well as Assistant Commissioner for IT integration and the national leader of our IT Solutions business line. He has proven abilities in producing business results, is highly committed to our customers, and has built an excellent relationship with our industry partners. We will make an excellent team, and I look forward to working with him as my deputy.”

As the Deputy Commissioner, Self will serve as the chief operating officer for FTS responsible for all day-to-day management and operations. “I will make the integration of the FTS business lines a top priority and I look forward to the unique challenges presented by the telecommunications industry,” Self said.

Since June 1997, under Self’s leadership, the FTS IT Solutions business line has provided more than $3 billion per year of nationwide technical and contractual assistance to federal agencies in all areas related to the acquisition, integration, development, management, and use of information systems and technology.

The IT Solutions business line is comprised of three nationwide programs: the Federal Systems Integration and Management Center (FEDSIM), the Federal Computer Acquisition Center (FEDCAC), and the Federal Acquisition Services for Technology (FAST) program, and 11 regional client support centers. Self directed the development of new business lines such as Seat Management, Smart Card, Financial Management Systems Services, and Fed Learn and was instrumental in the award of numerous multiple award contracts including ANSWER and Millennia.

Suda has been the FTS CFO since January 1998. He started with GSA in 1977 as an intern in the agency’s National Capitol Region. Since then, he has held numerous positions in the financial community in both the regional and headquarters offices. Prior to joining FTS, he was Director of Finance for GSA.

FTS has also selected Mike Norris as acting Chief Financial Officer and Mike McNeill as acting Chief Information Officer.

FTS provides information technology solutions that range from major systems integration to desktops and related support. It also provides advanced technology products and services including risk analysis and information security support, acquisition services for information technology and telecommunications systems, and office automation and network design.❖

(Courtesy of the General Services Administration)

## Level 3 Communications CEO James Crowe Assumes Chair of Network Reliability and Interoperability Council (NRIC)

Federal Communications Commission (FCC) Chairman William E. Kennard and Commissioner Michael K. Powell announced on March 6, 2000, that James Q. Crowe, President and Chief Executive Officer (CEO) of Level 3 Communications, Inc., will chair the next term of the Network Reliability and Interoperability Council (NRIC V).

Both Kennard and Powell thanked AT&T CEO C. Michael Armstrong for leading the Council during its previous term (NRIC IV).

The Council's members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations and government-related organizations.

The role of the Council is to develop recommendations for the Commission and the telecommunications industry to assure optimal reliability, interoperability and interconnectivity of, and accessibility to, public telecommunications networks. Last year, NRIC IV played a significant leadership role in telecommunications industry Y2K preparations.

Crowe has been CEO of Level 3 Communications since August 1997. He previously served as Chairman of the Board of WorldCom, Inc. from January to July 1997, and as Chairman and CEO of MFS Communications from 1986 through 1996. He is a director of three other telecommunications companies: Commonwealth Telephone in Pennsylvania; RCN Corporation, Princeton, New Jersey; and Inacom Communications, Inc., Omaha, Nebraska.

NRIC was first formed in January 1992 following a series of major telephone service outages and initially analyzed the causes of telephone service outages and recommended steps to avoid or mitigate such outages. In 1994, the Council's membership was expanded to include representatives of the satellite, cable television and wireless industries and it examined new reliability issues raised by the entry of new service providers and by changing telecommunications technologies.

In 1996, the Council developed recommendations for implementing Section 256 of the 1996 Telecommunications Act relating to oversight of joint network planning by telecommunications carriers and the development, by standards-setting organizations, of public telecommunications network interconnectivity standards.

More information about NRIC's activities and reports is available at its Web site at http://www.nric.org.❖

(Courtesy of the FCC)

## NSA Announces Centers of Academic Excellence in Information Assurance Education for 2000

The National Security Agency (NSA) has designated the following universities as Centers of Academic Excellence in Information Assurance Education. They join the list of seven universities across the country to be awarded this distinction.

The newly designated Centers of Academic

Excellence in Information Assurance Education are:

-Carnegie Mellon University,Pittsburgh, Pennsylvania;
-Florida State University, Tallahassee, Florida;
-Information Resources Management College, National Defense University, Fort Leslie J. McNair, Washington, D.C.;
-Naval Postgraduate School, United States Naval Academy, Annapolis, Maryland;
-Stanford University, Palo Alto, California;
-University of Illinois at Urbana-Champaign, Illinois; and
-University of Tulsa, Tulsa, Oklahoma.

Universities will be formally recognized during a presentation at the Fourth Annual Conference of the National Colloquium for Information Systems Security Education, which was held in the Doyle Hotel, Washington, D.C., May 23-25, 2000. For more information visit http://www.infosec.jmu.edu/ncisse.

The colloquium conference provides a forum for key figures in Government, industry, and academia to address current and emerging requirements in information assurance education, and to encourage the development and expansion of curricula, especially at the graduate and undergraduate levels.

Designations were granted following a rigorous review of university applications by review board members from NSA, industry, and academia. The board assessed applications against established criteria that measure the depth and maturity of information assurance programs, and are rooted in National Security Telecommunications and Information Systems Security Committee (NSTISSC) Training Standards. The NSTISSC is an intergovernmental organization that sets policy for the security of national security systems. For more information about the NSTISSC, please see http://www.nstissc.gov.

Last year, George Mason University, James Madison University, Purdue University, Idaho State University, Iowa State University, University of California at Davis, and the University of Idaho were named Centers of Academic Excellence in Information Assurance Education during the first annual program.

Universities receiving this distinction become eligible to participate in the Scholarship for Service (SFS) Program announced in the President's National Plan for Information Systems Protection, January 2000 (http://www.ciao.gov). Under the SFS Program, the Government pays for graduate or undergraduate studies meeting established information assurance standards, in return for a predetermined student commitment to Federal Government service.

The NSA established the Centers of Academic Excellence in Information Assurance Education Program in an effort to promote higher education in information assurance, and increase the number of individuals with this expertise. A June 1999 Department of Commerce Report, "The Digital Workforce," estimates that the United States will require more than 1.3 million new highly skilled information technology workers between 1996 and 2006.

***The U.S. will require more than 1.3 million new highly skilled information technology workers between 1996 and 2006.***

The National Plan for Information Systems Protection also addresses this critical shortage, and further highlights the acute shortage in the subset of trained information systems security personnel. The National Plan recognizes training and education as key solutions in defending America's cyberspace and establishes the Federal Cyber Services Training and Education Initiative to address the shortage. The Centers of Academic Excellence in Information Assurance Education Program is an example of the outreach and partnership efforts called for in the National Plan.

Additional information on the Centers of Academic Excellence in Information Assurance Education Program may be found at http://www.nsa.gov/isso. The program is managed by the Information Systems Security Organization of NSA, which provides the solutions, products and services, and conducts defensive information operations to achieve information assurance for information infrastructures critical to U.S. national security interests.❖

(Courtesy of the National Security Agency)