NSA'S NEW NATIONAL MISSION

by Vic Mathurin

President Reagan has responded to growing concern about the susceptibility of United States communications and computer systems to technical exploitation and to intelligence reports on the extent of the threat to these systems, by signing National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security."

NSDD 145, signed on September 17, directs a major reorganization of government COMSEC and computer security structures and expands the Agency's computer security mission, previously restricted to DoD, to a national responsibility.

The impetus for new policy is what the Directive cites as advances in microelectronics technology, unprecedented growth in telecommunications and information processing systems and the knowledge that technology to exploit these systems is used extensively by foreign nations and can be used by terrorist groups and criminal elements. The Directive also recognizes a fact long known to most of us—that information concerning the vital interests of the United States, even if unclassified in isolation, can reveal highly classified information when taken in aggregate.

Another reason for the recent flurry of government activity in the area of computer security may well be a growing public awareness regarding the vulnerability of data processed by computer, brought on, ironically, by the highly publicized escapades of computer "hackers."

Although the COMSEC Organization will be greatly affected by the new policy, the major impact will be on the DoD Computer Security Center, NSA's C Organization, and this article will focus on that aspect of the Directive.

The Center, which has been in existence less than four years, is still building an operation of the proportions required to protect DoD computer systems. With the bounds of military data lifted, the number of data processing systems to be protected becomes formidable. The new national Computer Security Center will be concerned with the data processing activities of over 1,000 federal departments, agencies, boards and commissions.

The task of assessing the scope of the mission is no small one. A year or more of study will be required. The Center has had few dealings with civil agencies, so new relationships will have to be established. What these agencies are using, what they are processing and what protection they need will have to be determined. The government has come to realize the critical nature of information concerning finance, agriculture, trade, energy, etc. and the Directive provides a mechanism for developing a program that will secure computers processing this kind of data.

The Center is expected to expand greatly as a result of NSDD 145. Research and Development (R&D) will be accelerated, and the computer security program will include funding for generic R&D tasks of other departments and agencies. To expand the national research base, cooperative R&D ventures with computer science graduate departments at leading universities will be sought. Commercial product and applications systems evaluations will increase dramatically. The focus will be on the Center's *Trusted Computer System Evaluation Criteria*, which codifies technical security measures designed into computer systems and allows government and industry to talk consistently on the subject for the first time. Vulnerability and threat programs, now in their infancy and limited to DoD systems, will have to encompass a prolific governmental computer structure. Training, education and the overall computer security awareness effort will also grow enormously. This means many more people, a lot more space and of course, more money.

SYSTEMS SECURITY STEERING GROUP

Secretary of State
Secretary of the Treasury
Secretary of Defense
Attorney General
Director, Office of Management and Budget
Director, Central Intelligence
Assistant to the President for National Security Affairs (Chairman)

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

Composed of a voting representative of each member of the Steering Group and each of the following:
Secretary of Commerce
Secretary of Transportation
Secretary of Energy
Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
Chief of Staff, United States Army
Chief of Naval Operations
Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System
Assistant Secretary of Defense for C^3I (Chairman)

The whole approach to assessing the degree of security required for specific applications will be affected. In the past, with highly classified data involved, emphasis was on acquiring the strongest protection measures available—defined in the *Criteria* as Verified Protection, the "A" Division. There are currently no systems at that level and when they are developed they will undoubtedly be expensive. Although a thorough study is yet to be made, it is highly likely that much of the data to be protected in the civil sector will require less stringent measures—systems that will be available in large numbers and will be relatively inexpensive—depending on the threat of exploitation and the potential damage to national security.

The NSDD actually goes beyond civil agencies. It includes encouraging, advising and assisting the private sector to identify systems handling sensitive non-government information; determining the threat to and vulnerability of these systems; and formulating strategies and measures for providing suitable protection.

Some idea of the dimensions of what NSA is being directed to do can be obtained from a look at the status of DoD systems. The Center conducted a survey to assess the current security posture of automated information systems handling classified and other sensitive DoD information. An analysis of the responses showed that a majority of the classified systems operate outside the region of acceptable risk. Add 1,000 agencies with presumably, similar conditions and segments of the private sector and we have a feel for the magnitude of what the Directive is attempting to accomplish when it states that systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured; and that systems handling other national security-sensitive, but unclassified, government or government-derived information shall also be protected.

The first step toward accomplishing this is reorganization. NSDD 145 establishes a senior-level Systems Security Steering Group, a National Telecommunications and Information Systems Security Committee at the operational level, an Executive Agent and a National Manager (the Director of NSA).

The Committee will have two subcommittees. One will focus on telecommunications security and will be chaired by Dr. Robert

Conley, Assistant Secretary for Electronic Systems and Information Technology, Department of the Treasury. The second, concerned with automated information systems security, will be chaired by the Director of the Computer Security Center.

DIRNSA will function as executive secretary to the Steering Group and will provide a permanent secretariat to the Committee and the two subcommittees.

The Committee will operate under the direction of the Steering Group and the Director of NSA, as National Manager, will act for the Executive Agent.

By authority of Executive Order 12333, the Secretary of Defense is Executive Agent for COMSEC. NSDD 145 expands his role to telecommunications and automated information systems security under the following definitions.

Telecommunications: the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

Automated Information Systems: systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, including computers, word processing systems, other electronic information handling systems and associated equipment.

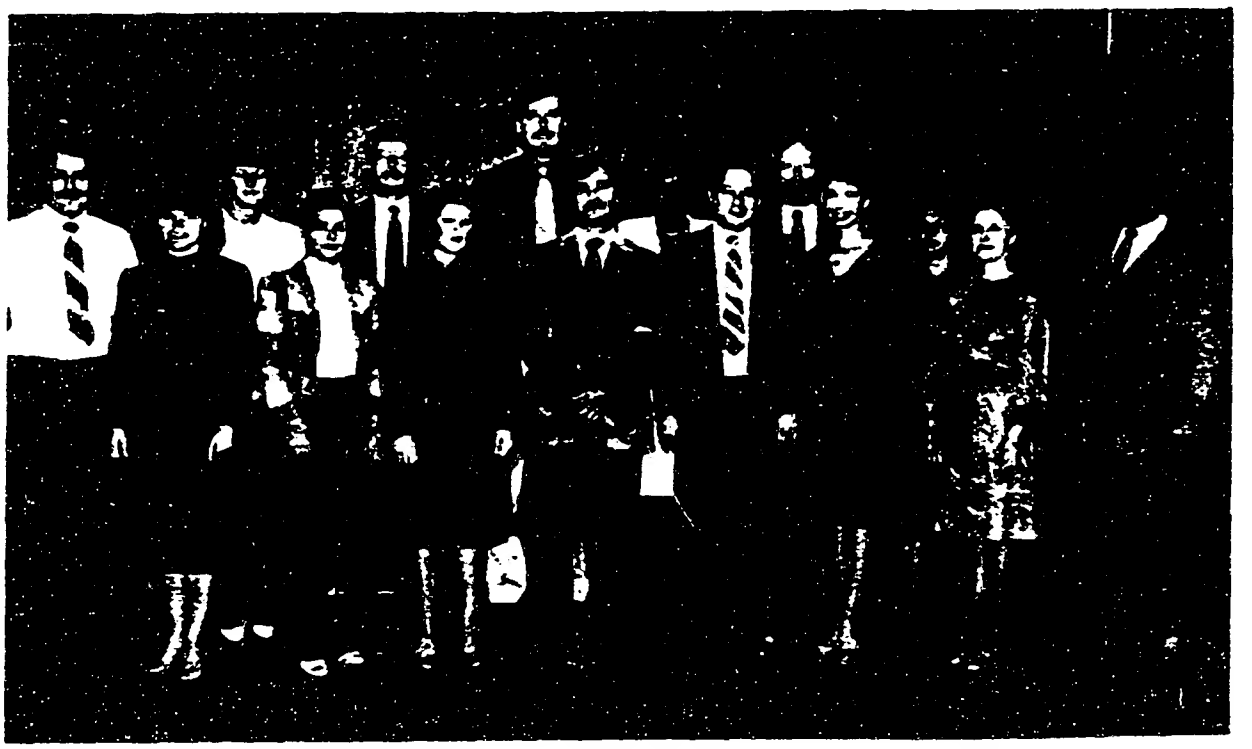
In fulfilling the responsibilities of the Executive Agent, the National Manager's tasks include, among others, determining the vulnerability of and hostile threat to government (and certain other) systems; evaluating and certifying the security of these systems; and conducting R&D and foreign liaison.

This is no simple set of tasks, but it is an interesting challenge and plans for expansion are already under way. The demands are great, but they derive from a confidence in the Agency and bring with them the opportunity to prove again our capacity to respond to critical situations affecting the national security.

Because the *Newsletter* contains information about NSA employees and activities which has not been made available to the general public, reasonable care must be taken to keep it within the circle of Agency employees, retirees, and immediate families. *Newsletter* copies received in the mail or taken from Agency buildings should be given special care and should be destroyed as soon as they have been read. All *Newsletters* distributed to Agency facilities outside the Fort Meade/FANX Complex are distributed FOR OFFICIAL USE ONLY and may not be taken outside of the facilities.

Tech Track Experts Ponder New Programs—As members of the Technical Track Implementation Group (TTIG), several of the Agency's Senior Technical Experts advise on issues of interest to technical people. The TTIG is working with the National Cryptologic School (NCS) on ideas to improve technical training opportunities. Tom Cindric, NCS Representative, has proposed some interesting programs for the group to consider. Pictured here, from left to right, are Chuck Steinecke, TTIG Chairman; K. Speierman, Chief Scientist; Randy Baker, Technical Track Program Director; and TTIG members Jack Jones, Ned Neuberg, Jack Mortick, Tom Cindric and Wayne Stoffel. Other members who are not pictured are Alice Dibben and John Taggart.

FY85 Civilian Welfare Fund Council Members



1st row: Mary Lou Van Newkirk, Katherine S. Nakamura, Helen K. Cleveland, James M. Gick, Michael B. Feldblum, Elizabeth Gerheiser, Jessie M. Goggin, Earl E. Warren
2nd row: Larry W. Bowers, Dawn L. Bailey, Daniel Knauf, Willard W. Wilt, Ann Bostic, Scott Snyder, Darlene W. Pencek