1270

496233

ND011-01

Cm009

FG013

LE

FG006-12

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

WS

February 25, 1987

MEMORANDUM FOR JAMES C. MURR

FROM: GRANT S. GREEN, JR. Bob for

SUBJECT: DOD Testimony on H.R. 145 -- Computer Security Act

The NSC Staff has reviewed the proposed DOD testimony and clears on the text as submitted.

NSC# 8701270

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

February 25, 1987

ACTION

MEMORANDUM FOR GRANT S. GREEN, JR.

FROM: BARRY KELLY

SUBJECT: DOD Testimony on H.R. 145 -- Computer Security Act

At Tab I for your signature is a memo to James Murr providing NSC clearance on DOD testimony on H.R. 145. The testimony will be given at a hearing before the Transportation and the Science Subcommittee of the House Science Committee.

John Grimes, Alison Fortier, Paul Stevens and David Major concur.

PREPARED BY: JAMES F. COLLINS

RECOMMENDATION

That you sign the memorandum to OMB at Tab I.

Approve _____ Disapprove _____

Attachments
Tab I Memo to OMB
Tab II Incoming Correspondence

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

SPECIAL

February 24, 1987

SPECIAL

LEGISLATIVE REFERRAL MEMORANDUM

TO: Legislative Liaison Officer

Department of Commerce- Joyce Smith (377-4264)
Department of Energy - Bob Rabben (586-6718)
Department of Justice - Jack Perkins (633-2113)
Department of State - Lee Ann Howdershell (647-4463)
Department of the Treasury - Carole Toth (566-8523)
Office of Personnel Management - Jim Woodruff (632-5524)
Department of Health & Human Services - Fran White (245-7750)
General Services Administration
National Security Council
Central Intelligence Agency

SUBJECT: Department of Defense testimony on H.R. 145 -- Computer Security Act for a hearing before the Transportation and the Science Subcommittee of the House Science Committee.

(NOTE -- The testimony by Lt. Gen. Odom sent to you earlier today is different and is directed to a House Government Operations Subcommittee.)

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than

10:00 a.m. -- WEDNESDAY -- FEBRUARY 25, 1987

Questions should be referred to Constance J. Bowers (395-3457), the legislative analyst in this office.

James C. Murr for
Assistant Director for
Legislative Reference

Enclosures

cc: Ed Springer, Arnold Donahue, Kevin Scheid, John Cooney, Greg Henry, Bob Bedell, Jack Carley

STATEMENT BY

LIEUTENANT GENERAL WILLIAM E. ODOM, USA

DIRECTOR

NATIONAL SECURITY AGENCY

AND

NATIONAL MANAGER

NATIONAL TELECOMMUNICATIONS AND AUTOMATED INFORMATION

SYSTEMS SECURITY

CONCERNING H.R. 145

BEFORE THE

SUBCOMMITTEE ON

TRANSPORTATION, AVIATION, AND MATERIALS

AND THE

SUBCOMMITTEE ON

SCIENCE, RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

FEBRUARY 26, 1987

Mr. Chairman and members of the subcommittees:

Thank you for the opportunity to appear before you and to present my views on H.R. 145, the Computer Security Act of 1987. I am of the view that the attention being paid to computer security by your subcommittees, the full Science, Space, and Technology Committee, and the House Committee on Government Operations have done a great deal to raise the awareness of not just Federal employees, but the American public at large, that computer security is a national problem. I thank you for that help in raising everyone's consciousness, and hope we can work together to find solutions to the problem.

I am concerned, however, that the proposed legislation at hand, as it is currently drafted, does not lend itself to a unified, government-wide, national approach to the issues of computer security. I see in the legislation many similarities between it and the version of H.R. 2889 that the Committee on Science and Technology reported to the House floor in August of last year. And in reviewing the report that accompanied H.R. 2889 I see that, notwithstanding the extensive hearings that were held on that bill, there remain some fundamental misunderstandings about what NSDD 145 accomplishes, and NSA's role in the NSDD 145 process.

The report claims that,"[a]lthough NSA has a fine track record as the lead technical agency for securing ADP systems containing national security data, it is not clear that it is the appropriate lead agency for directing civil agency computer security." The report points out that "NSDD-145 can be

interpreted to give the national security community too great a role in setting computer security standards for civil agencies," and calls for "a civilian authority . . . to develop standards relating to sensitive, but unclassified data." The report alleges that the composition of the interagency committee created by NSDD-145, the National Telecommunications and Information Systems Security Committee (NTISSC) "favors military and intelligence agencies." The report points up a need for "greater emphasis [to] be given to cooperation between the military and civil agencies as well as the private sector in setting computer security and training goals," and states that this can be accomplished by "fostering greater communication and cooperation between the NBS and NSA in setting overall Federal computer [sic] policy."

First of all, let me say that the communication and cooperation that already exists between the National Security Agency and the National Bureau of Standards could serve as a model for the rest of our government. It is a well-traveled two-way street between Fort Meade and Gaithersburg. We are currently negotiating a formal, detailed Memorandum of Agreement that reflects and enhances our current, ongoing cooperative relationship in the field of Information Security. The agreement that we are negotiating outlines the responsibilities of and interrelationship between the National Bureau of Standards and the National Security Agency in implementing the requirements of NSDD 145 to secure automated information systems processing classified or sensitive, but unclassified, government or

government-derived information; to protect federal government operated automated information systems processing information which is neither classified nor sensitive within the meaning of NSDD 145; and to assist the private sector in protecting its automated information systems processing information the private sector may choose to protect.

Our fine relationship with the National Bureau of Standards in the field of computer security, in fact predates NSDD 145 by a good many years, and we have worked together over the years to solve technical issues of common concern.

This fall, for example, we will be co-sponsoring with the National Bureau of Standards for the tenth time, our joint annual National Computer Security Conference. This conference is clearly the standard by which other computer security conferences are judged, with attendees from private industry and governments around the world. In fact, the conference is so successful that it has outgrown the facilities at Gaithersburg, where it was held up until last year, and this year it will be held at the Baltimore Convention Center. Incidentally, Mr. Chairman, I would like to take this opportunity to personally invite you and your colleagues to attend this year's conference so you can see for yourselves, firsthand, the fine cooperation and communication that currently exists between the NSA and the NBS.

NSA and NBS are also currently very heavily involved in planning and executing computer security research and development; planning and conducting computer security training and awareness activities; participating in network security

methodology and evaluation criteria development; and developing risk analysis methodology.

And Mr. Chairman, our cooperation with the National Bureau of Standards is by no means bilateral. NBS and the Director of the Bureau's Institute for Computer Science and Technology have, virtually since the inception of the NTISSC, and its Subcommittee on Automated Information Security (SAISS), played a key role on those bodies. The Director of the ICST has served, almost from the time the SAISS was created, as the Chairman of the SAISS Working Group that is responsible for publishing NTISSC standards, criteria, and guidelines.

The National Computer Security Center, established at the National Security Agency shortly after the President expanded the scope of its mission from its previous role as the DoD Computer Security Center when he signed NSDD 145, has made giant strides and a tremendous effort to meet the needs of the civil sector component of its expanded constituency.

As part of this effort, during August 1985, letters were sent to the heads of 79 organizations throughout the Federal government, including independent government establishments and government corporations, offering computer security assistance, outlining the services offered by the Center, and requesting a point of contact for computer security matters. A team from the National Computer Security Center visited these organizations between August 1985 and July 1986 to introduce them to the Center's mission, to discuss the need to protect sensitive data,

and to make them more aware of the security measures available to protect sensitive data. The response from those agencies was very enthusiastic.

A separate branch has been established within the National Computer Security Center to support the civil sector of the government. The branch provides the following services:

Computer Security Enhancement Reviews - These programs consist of short-term (two days to one week) on-site technical analyses. They identify threats and vulnerabilities, provide an outbrief report of these vulnerabilities, and recommend methods to reduce the vulnerabilities. Computer Security Enhancement Reviews are in progress or have been completed at 11 civil departments and agencies.

Technical Consultations - These consultations provide a variety of support services, from discussions on a particular area of customer concern, to a one-time review visit. The one-time review visit is not as detailed as a Computer Security Enhancement Review visit, nor does it provide as much detail. It provides a very short review of the vulnerability of a system. Technical consultations are in progress or have been completed at 21 civil departments and agencies.

Request for Proposal (RFP) Security Review for Trusted Systems - This security review consists of assisting the customer with incorporating security

requirements in the procurement process. Such security reviews are in progress or have been completed at eight civil agencies.

Security Policy Review - This takes the form of providing consulting assistance to customers during the drafting of computer security policy. A security policy review is in progress or has been completed at 14 civil departments and agencies.

In addition, beginning in May 1986, the Center embarked on a program, at the behest of the SAISS, aimed at familiarizing the civil sector with the applicability of the Center's Trusted Computer System Evaluation Criteria. I had issued the Criteria, in my role as National Manager, as a National Telecommunications and Information System Security Advisory Memorandum. Over forty civil departments and agencies took advantage of the training, and the Center is using information gained from those civil agencies during the course of the training to revise and update the Criteria, thus making it more applicable to the computer environments of those civil departments and agencies. When that job is finished, the NTISSC plans to issue the Criteria as an NTISS Instruction.

The National Computer Security Center has also published numerous computer security guidelines, standards, informational brochures, posters, leaflets, and videotapes. These have been distributed variously throughout the civil sector of government, private firms, and the academic community. Nearly 1100 copies of the videotape alone have been distributed in a year and a

half. I have brought copies of these publications with me for inclusion in the record of these hearings, and am providing you with copies of the videotapes so you may view them.

Are our efforts showing results? We believe that indeed they are. Let me provide three brief examples. They demonstrate how the National Computer Security Center has been assisting the Department of State, the Department of the Treasury, and the Federal Aviation Administration with developing Requests for Proposal (RFPs) to industry for trusted computer systems worth several billion dollars over the life of the contracts.

Last fall, the State Department released their RFP entitled "ADP Equipment and Services," with an estimated value greater than $400 million over a contract life of five years. After the RFP was released, the State Department was challenged by some vendors on the security requirements of the proposal that specified a "B2" level of trust. Basically, the vendors were claiming that a "B2" system would not be technically achievable in the time specified. The National Computer Security Center held a number of discussions with State Department officials. The talks included reviews and detailed discussions on the very sensitive information processed on State Department systems, the extremely hostile environment at some U.S. embassies, and the technical rationale behind specifying a "B2" level of trust for the systems in question. The Center also briefed the State Department on the status of vendors who are developing trusted products that would meet the Department's requirements. The State Department subsequently made the decision to leave the RFP

as written. The National Computer Security Center will assist State in the technical review of proposals received from industry.

Moreover, the Treasury Department has released an RFP on the Treasury Minicomputer Acquisition Contract (TMAC) for comment. Treasury is planning to formally release the RFP in March or April. The TMAC will span a five-year period for the purchase of minicomputers throughout the Department, with the Internal Revenue Service being the primary beneficiary. The contract is estimated to be valued in excess of $600 million. Following the strategy of the draft policy in the NTISSC that is proposing the requirement for Controlled Access Protection (CAP), Treasury took the initiative to specify the CAP or "C2" level of trust as a minimum security specification. As a highly desirable feature that will receive additional credit, the "B2" level of trust was also specified. The National Computer Security Center drafted the security specifications for the RFP, and will be supporting Treasury in the technical review of the responses received from industry.

Under an interagency agreement with the Federal Aviation Administration, the National Computer Security Center has committed resources to provide a year-long effort to improve the computer security posture throughout the FAA. This included a study of the current Air Traffic Control System, a study of the interim host system, and an evaluation of the design specifications for the planned $11 billion Advanced Automation System. Work on this last system resulted in significant input

to the developing RFP, the initial security policy for the system, and most significantly, setting the level of trust at the C2 level for hardware and software associated with the Advanced Automation System--steps that we believe will positively affect the safety of millions of future air travelers.

A little over a year ago, the National Computer Security Center moved into a facility close to Baltimore-Washington International Airport. We are making every effort there to make our laboratories and facilities state-of-the-art and second to none--as befits a national center of excellence. I should like to extend an open invitation for you to visit the Center and see firsthand for yourselves what we are doing. We currently have slightly over 300 people on board at the Center, and are actively recruiting to meet an authorized strength of nearly 350 people.

We at NSA have clearly made a significant investment in information security, and believe we have been responsible stewards of the funds you in the Congress have allocated, authorized, and appropriated to us over the years for information security purposes and for the good of the nation. I would hope that my testimony today helps to persuade you that the criticisms of NSA and the NSDD 145 structure that appeared in the report of the Committee on Science and Technology which accompanied H.R. 2889 were unfair and not justified.

We believe that, in a very short period of time, we have ably demonstrated that we can, indeed, serve the civil sector of our government just as well as we have our more traditional customers. We at the National Security Agency take pride in our

role as a truly national agency, and look forward to further opportunities to expand our "fine track record as the lead technical agency for securing ADP systems," as your committee report so generously describes.

Thank you again for the opportunity to testify before you. That concludes my prepared statement. I would be happy to answer any questions you may have.