1955

498500

ND 011-01

UT001

FG006-12

THE WHITE HOUSE

WASHINGTON

March 24, 1987

MEMORANDUM FOR LIEUTENANT GENERAL WILLIAM E. ODOM
Director, National Security Agency

SUBJECT: Cancellation of NTISSP 2, National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems

In your capacity as Executive Secretary of the Systems Security Steering Group, you are hereby requested to circulate for coordination and concurrence the attached memorandum to all members of the Systems Security Steering Group.

Frank C. Carlucci

Attachment
Proposed Memorandum to
Recipients of NTISSP 2

NSC# 8701955

DRAFT

MEMORANDUM FOR (ALL RECIPIENTS OF NTISSP 2)

SUBJECT: Cancellation of NTISSP 2

Policy Directive NTISSP 2, National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, issued October 29, 1986, is hereby cancelled.

FOR THE SYSTEMS SECURITY STEERING GROUP:

William Odom
Executive Secretary

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

March 18, 1987

ACTION

MEMORANDUM FOR FRANK C. CARLUCCI

FROM: BARRY KELLY BK

SUBJECT: H.R. 145: Cancellation of Policy Directive NTISSP 2

On March 12, 1987, you informed Congressman Brooks that the Administration was setting in motion the procedures and paperwork to rescind NTISSP 2, the policy directive on Sensitive, but Unclassified information issued on October 29, 1986 by John Poindexter as Chairman of the Systems Security Steering Group.

The most appropriate means for rescinding the directive without placing you in the position of issuing a directive as SSSG Chairman, is to have the SSSG Executive Secretary, Lt General Odom do so on behalf of the SSSG.

At Tab I is a memorandum from you to General Odom asking him, in his capacity as Executive Secretary of the SSSG, to seek concurrence from the SSSG members for a memorandum cancelling NTISSP 2. Paul Stevens, Alison Fortier and Will Ball concur.

PREPARED BY: JAMES F. COLLINS

RECOMMENDATION

That you sign the memorandum to General Odom at Tab I.

Approve _____ Disapprove _____

Attachments
Tab I Memo to General Odom
A Draft Memo to Recipients of NTISSP 2
Tab II Ltr to Chairman Brooks, dtd March 12, 1987
Tab III NTISSP 2

THE WHITE HOUSE

WASHINGTON

March 12, 1987

Dear Mr. Chairman:

I am writing about your concerns over Administration policy in the area of computer security.

I understand you have raised the issue of whether the structure outlined by the President in NSDD 145 assigns a proper role to the National Security Adviser by designating him to serve as Chairman of the Systems Security Steering Group. I also understand you have concerns about provisions of policy directive NTISSP 2, issued by my predecessor John Poindexter as Chairman of the Systems Security Steering Group.

The issues you have raised are matters of legitimate and important concern. I have directed my staff to review immediately NSDD 145 and policy directive NTISSP 2. In that review they will include as a key objective finding a mechanism to eliminate any possible ambiguity regarding the role of the National Security Adviser in connection with the Systems Security Steering Group.

With respect to NTISSP 2, I have instructed my Staff to initiate the procedures and prepare the papers necessary to rescind that document.

I will inform you about the results of these actions as soon as they are completed.

Sincerely,

Frank C. Carlucci

cc: The Honorable Frank Horton

The Honorable Jack Brooks
Chairman
Committee on Government Operations
U.S. House of Representatives
Washington, D.C. 20515

NTISSP No. 2
29 October 1986

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

NATIONAL POLICY

ON

PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SSSG
SYSTEMS
SECURITY
STEERING
GROUP

CHAIRMAN

FOREWORD

NSDD-145, "National Policy on Telecommunications and Automated Information Systems Security," signed by the President on 17 September 1984, in part provides policy and direction for systems protection and safeguards for telecommunications and automated information systems that process or communicate sensitive but unclassified information. The NSDD-145 Systems Security Steering Group has established that sensitive, but unclassified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however, the determination of what is sensitive, but unclassified information is a responsibility of Agency heads. Executive Order 12356 prescribes requirements for classifying, declassifying, and safeguarding national security information.

This policy and the principles and procedures contained in Office of Management and Budget (OMB) Circulars Nos. A-123 and A-130, "Management of Federal Information Resources," are complementary.

John M. Poindexter

NATIONAL POLICY
ON
PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information will protect such information to the level of risk and the magnitude of loss or harm that could result from disclosure, loss, misuse, alteration, or destruction.

SECTION II - DEFINITION

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information.

SECTION IV - RESPONSIBILITIES

This policy assigns to the heads of Federal Government Departments and Agencies the responsibility to determine what information is sensitive, but unclassified and to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems. The Director of Central Intelligence shall, in addition, be responsible for identifying sensitive, but unclassified information bearing on intelligence sources and methods and for establishing the system security handling procedures and the protection required for such information.

Federal Government Department and Agency heads shall:

a. Determine which of their department's or agency's information is sensitive, but unclassified and may warrant protection as sensitive during communications or processing via telecommunications or automated information systems. This determination should be based on the department's or agency's responsibilities, policies, and experience, and those requirements imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted;

b. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information requiring protection;

c. Determine, in coordination with the National Manager, as appropriate, the threat to and the vulnerability of those identified systems and;

d. Develop, fund and implement telecommunications and automated information security to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

e. Ensure implementation of telecommunications and automated information systems security consistent with the procedures and safeguards set forth in OMB Circular A-123 and A-130.

The National Manager shall, when requested, assist Federal Government Departments and Agencies to assess the threat to and vulnerability of targeted systems, to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.