TJ

THE WHITE HOUSE

WASHINGTON

CJ

July 1, 1986

4648 437529

ND011-01
CMD09
LLT001
FG011
FG012
FG017
FG006-11

MEMORANDUM FOR LIEUTENANT GENERAL WILLIAM E. ODOM
National Manager, NTISS

THE HONORABLE DONALD C. LATHAM
Chairman, NTISSC

THE HONORABLE RONALD I. SPIERS
Under Secretary of State for Management

MR. ROBERT M. KIMMITT
General Counsel
Department of Treasury

MR. JOHN N. RICHARDSON
Senior Special Assistant to the
Assistant to the Attorney General
and Chief of Staff
Department of Justice

MR. PHILIP A. DUSAULT
Acting Associate Director
National Security and International Affairs,
OMB

VICE ADMIRAL EDWARD A. BURKHALTER
Director
Intelligence Community Staff

SUBJECT: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

At the first NSDD-145 SSSG Meeting in December, 1985, the Chairman, NTISSC was instructed to prepare a comprehensive policy for the protection of sensitive, but unclassified information handled by Federal Government telecommunications and automated information systems and to leave the determination of what is sensitive to national interests to the heads of Government Departments and Agencies, and entities.

The enclosed draft policy statement for sensitive, but unclassified information prepared by the NTISSC, is forwarded for your review and comment. Request your concurrence and/or comments by July 15, 1986.

Rodney B. McDaniel
Executive Secretary
National Security Council

Attachment
Tab A Draft Policy

IDC 8604648

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 that information to the level of threat of exploitation and the associated potential damage to the national interests. The Federal Government is also required to protect those systems which communicate or process personal and financial data provided to it by its citizens as well as company proprietary information while in the possession of U.S. Government Departments and Agencies and entities.

SECTION II - DEFINITION

Sensitive, but unclassified government information is information, the loss, misuse, destruction, or the unauthorized manipulation or alteration of which during its telecommunications or processing via federal government communications or automated information systems, could adversely affect the national interests, citizens, and commercial business of the United States. National interests include, but are not limited to, the wide range of economic, human, financial, industrial, agricultural, technological and law enforcement government information and assets of the United States in addition to national defense and foreign relations matters.

SECTION III - APPLICABILITY

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

SECTION IV - RESPONSIBILITIES

This policy assigns the responsibility to the heads of Federal Government Departments and Agencies for determining what information is sensitive, but unclassified; and for providing systems protection of such information which is electronically communicated, transferred, processed, or stored on government communications and automated information systems.

Federal Government Department and Agency heads shall:

a. Determine which of their Department's or Agency's information is sensitive, but unclassified.

b. Identify those categories of information they generate and those categories of information they obtain from the public which warrant protection as sensitive during their communication or processing via government telecommunications or automated information systems. This determination should be based on the Department's or Agency's responsibilities, policies, and experience, and those imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted.

c. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information.

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

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

The National Manager shall provide guidance and assistance to Government Departments and Agencies to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

June 16, 1986

ACTION

MEMORANDUM FOR JOHN M. POINDEXTER

FROM: JOHN G. GRIMES/KEN DEGRAFFENREID

SUBJECT: Proposed Policy: "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems"

The NSDD-145 Senior Security Steering Group (SSSG) which you chair, agreed at its first meeting December 20, 1985, that the NTISSC should prepare a policy statement on what is sensitive, but unclassified information that should be protected when handled/processed by Federal Government telecommunications and automated information systems.

At Tab B the Secretary of the SSSG, Bill Odom, has forwarded to you this proposed policy statement with two options: Concurrence or forwarding to other Steering Group members for review and comment. Even though the policy statement has been prepared and concurred in by the NTISSC, it should be reviewed by the SSSG members. This is an important policy with potential for being raised on the Hill. We have made some minor changes and corrections to the proposed policy statement for clarification and consistency of terms.

Attached at Tab II in a short note from you to Bill indicating that you are giving this statement one more time around the circuit.

RECOMMENDATION

As Chairman of the SSSG, that you sign the memorandum at Tab I forwarding the proposed policy on sensitive, but unclassified information to the SSSG members for review and comment. Also, that you sign the cover note to Bill Odom at Tab II.

Approve _____ Disapprove _____

Attachments

Tab I Memorandum to SSSG Members
Tab II Cover Note to Bill Odom
Tab A Proposed Policy
Tab B Memorandum from LTG Odom

NTAISS
NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY

NATIONAL MANAGER

NTISS-004/86
12 May 1986

MEMORANDUM FOR THE CHAIRMAN, SYSTEMS SECURITY STEERING GROUP

SUBJECT: Proposed Policy - "Protection of Sensitive, But Unclassified Information in Government Telecommunications and Automated Information Systems"

I am forwarding with this memorandum, a proposed National Telecommunications and Information Systems Security Policy prepared by the NTISSC at the direction of the Steering Group. The Steering Group unanimously agreed, at their 20 December 1985 meeting, that the intent of NSDD 145 is to address a broader and comprehensive meaning of sensitive, but unclassified information and to leave the determination of what is sensitive to each government department and agency head.

The NTISSC policy proposal incorporates the Steering Group's guidance and properly reflects the intent of NSDD 145. I have enclosed a foreword for your release, should you elect to do so, or if you prefer, I shall forward the policy to the Steering Group members for a final review.

I recommend your endorsement.

Wm E Odom
WILLIAM E. ODOM
Lieutenant General, USA

Encl:
a/s

Chairman Decision:

CONCUR:_____

FORWARD TO THE STEERING
GROUP MEMBERS:_____

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, directs that certain protection be developed and provided for U.S. Government telecommunications and automated information systems which handle classified information and sensitive, but unclassified information. Executive Order 12356 prescribes a system for classifying, declassifying, and safeguarding national security information. NSDD 145 recognizes that, in addition to classified information, the government also handles sensitive, but unclassified information which should be protected. At its 20 December 1985 meeting, the Systems Security Steering Group agreed that the intent of NSDD 145 is to address a broader and more comprehensive meaning of sensitive, but unclassified information, and that the determination of what is sensitive information is the responsibility of each department and agency head. This policy, devoted to national interests information, and Office of Management and Budget Circular No. A130, "Management of Federal Information Resources," are complementary in covering information requiring protection.

JOHN M. POINDEXTER
Vice Admiral, USN

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

SECTION I - POLICY

Government departments and agencies shall protect telecommunications and automated information systems handling sensitive, but unclassified information. These systems shall be protected in proportion to the threat of exploitation and the associated potential damage to the national interest. The government also is committed to taking positive steps to protect personal and financial data provided to it by its citizens and to protect company proprietary information it obtains.

SECTION II - DEFINITION

Sensitive, but unclassified information is information, the loss, misuse, destruction, or the unauthorized manipulation or alteration of which could adversely affect the national interests of the United States. National interests include, but are not limited to, the wide range of economic, human, financial, industrial, agricultural, technological and law enforcement assets of the United States in addition to national defense and foreign relations matters.

SECTION III - APPLICABILITY

This policy applies to all government departments, agencies and contractors which electronically transfer, store, process, or communicate sensitive, but unclassified information.

SECTION IV - RESPONSIBILITIES

This policy assigns the responsibility to the heads of government departments and agencies for determining what information is sensitive, but unclassified; and for identifying and protecting those systems which electronically communicate, transfer, process, or store such information.

Government department and agency heads shall:

a. Determine which of their department's or agency's information is sensitive, but unclassified;

b. Identify those categories of information they generate and those categories of information they obtain from the public which warrant protection as sensitive. This determination should be based on the department's or agency's responsibilities, policies, and experience, as well as National Manager guidance on areas that potential adversaries have targeted.

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

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

e. Develop a communications and computer security program, to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security requirements.

The National Manager shall provide guidance and assistance to government departments and agencies to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.