NSTISSC-034-99
26 April 1999

POSITION PAPER ON

INFORMATION ASSURANCE (IA)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

National Security Telecommunications and Information Systems Security Committee

CHAIRMAN

NSTISSC-034-99

MEMORANDUM FOR MEMBERS AND OBSERVERS OF THE NSTISSC

SUBJECT: INFORMATION ASSURANCE POSITION PAPER

1. Attached, for your information and retention, is the approved version of the "NSTISSC Position Paper on Information Assurance," dated April 1999. As noted, this paper was produced by the NSTISSC Information Assurance Issue Group (NIAIG) under the Chairmanship of Mr. Thomas Burke from the General Services Administration.

2. This is an excellent thought paper and, as we prepare to enter the 21st Century, should serve to sensitize the NSTISSC membership to changing directions in the area of Information Assurance (IA). At a minimum, the paper should provide some modicum of direction for the follow-on efforts that will be necessary to respond to the significant IA challenges of the future.

Arthur Money

(b) (6)

Encl:
a/s

Copy Furnished:
SISS/STS Members & Observers

NSTISSC Secretariat [redacted] • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716

(b) (3)-P.L. 86-36

SECTION I - PURPOSE

1. This position paper is intended to promote development of information assurance policy by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This paper was produced by the NSTISSC Information Assurance Issues Group (NIAIG). It provides a strawman interagency plan of action to promote information assurance by the NSTISSC.

SECTION II - BACKGROUND

2. The advent of the Information Age, with information technology evolving at an extraordinary pace, is dramatically transforming the way government and, for that matter, society at large think about information. It is also transforming the way the government and the economy function. Both are increasingly dependent on information and data that is either transported on or stored in computers or computer controlled networks and infrastructures. As the basis for wealth transitions from labor to information, information is viewed in much the same way as industrial capital and capacity. It has value, it enables, it is a target in and of itself, it can be changed, stolen, or destroyed. Therefore, it must be protected. There are three trends that have an effect on the vulnerability of national security systems and information:

- Information Technology. In the Industrial Age, people talked to people. As the transition to the Information Age began, people talked to computers. Now computers are talking to computers.

- Threat. During the cold war, the threat was more monolithic, mostly focused on physical destruction. In the Information Age, it is much more diffuse with information bombs potentially having the same or greater impact than explosive bombs.

- Decentralization of Decision Making and Control. Information technology advances have resulted in flattened organizations and decentralized management control over decision making processes. Such scenarios create significant new challenges in the context of identifying, addressing, and correcting known vulnerabilities.

These trends have profound implications for the national security community:

a. National security information (as defined in Executive Order (E.O.) 12958) travels extensively in electronic form on commercial infrastructures, as well as on government owned and operated systems. Thus, the information infrastructure used for the Department of Defense and national security information is the same infrastructure used for most other types of electronically transmitted information.

b. While both government and the nation at large demand the speed, availability, and connectivity afforded by open interconnected networks, information in its digital form is vulnerable to a wider range of threats in significantly different ways than it is in its hard copy form.

c. Network interconnection produces vulnerabilities that encompass a wider pool of potential adversaries. They range from amateur hackers who can download intrusion tools off the Internet, to digitally smart common criminals, to terrorists and international criminals, and to foreign nations. They may mount a digital attack against national security information, but they are likely to do so through the shared global infrastructure in which large volumes of information reside. They may also mount an attack against a computer-controlled infrastructure which does not contain national security information, for example, the electric power grid or the air traffic control system. The damage from such an attack, particularly one that is sophisticated and large scale, could have dramatic national security consequences.

d. The level of investment by a digital attacker is insignificant compared to the level of damage that can be done.

e. A digital attack on either national security systems or unclassified systems can have serious national security consequences. For that reason, information assurance for both kinds of systems must be considered with the context of existing authorities (e.g., NSD-42, the Computer Security Act, OMB Circular A-130, etc.).

f. Because national security information is extensively transmitted and resident on a globally interconnected infrastructure, formerly self-contained national security community sanctuaries are increasingly at risk. Therefore, this community must look outside itself for solutions to protect national security information. In the future, it is expected that both civil government agencies and the private sector will play an expanded and, as yet, undefined role in protecting national security information. Increasingly, the security of national security information may be as much a function of how the national security community can influence and work with other communities to reduce overall risks and vulnerabilities, rather than merely deciding how to protect information falling under its authorities.

g. The need for protection of national security information may no longer by accurately measured solely in the context of levels of classification. Information, in and by itself, may have inherent value that requires protection. This change calls into question the relevancy of the current definition of national security information, because it may inappropriately constrain the policy and processes necessary to achieve information assurance.

h. Because the global information infrastructure is interconnected and the pace of technology evolution is so rapid, simply understanding the extent of vulnerabilities is a monumental task and an important first step in identifying appropriate information assurance solutions. Absolute information assurance may not be possible in an interconnected world. Risk management will become increasingly important and necessary.

3. The President's Commission on Critical Infrastructure Protection (PCCIP) met for over a year to examine these types of problems. Presidential Decision Directive (PDD-63), Critical Infrastructure Protection, was subsequently issued and serves to establish a framework for addressing critical infrastructure vulnerability issues. The NSTISSC should posture itself as a resource to be engaged and used within the context of PDD-63 and should seek an active role in implementing recommendations deriving from the established framework.

SECTION III - PROPOSED NSTISSC INFORMATION ASSURANCE POSITION

4. Information assurance is the protection of information in information systems by ensuring its availability, authenticity, confidentiality and its integrity. Information assurance encompasses detection, reaction and restoration capabilities, and it also seeks to guarantee the non-repudiation of transactions among information systems and their users.

5. In furthering Information Assurance objectives:

a. The NSTISSC recognizes that many of the solutions for protecting national security systems and information reside outside the national security community. It will work within existing legal and policy frameworks and avail itself of the interagency process to define an appropriate complementary role for itself in the context of the PDD-63. Its objectives should be to develop a strategy for influencing both civil agency and private sector information assurance policies and developments in ways that will provide necessary and cost-effective protection for national security information and critical infrastructures.

b. The NSTISSC will sponsor a review of the relevancy of the terms "national security systems" and "national security information" in response to the realities of today's globally interconnected networks whereby these systems and information, as traditionally defined, are difficult to segregate from other information and networks. Policy recommendations will be developed and disseminated for consideration within the interagency framework.

c. The NSTISSC recognizes that understanding the extent of

vulnerabilities with respect to specific systems in a networked environment is a significant challenge. It will promote the application of both existing and new risk assessment and risk management models for national security systems; support risk assessment research and development efforts; and encourage security assessments of identified high-risk systems.

d. The NSTISSC will investigate and promote the use of metrics as a tool for assessing the value of national security information and quantifying the investments necessary to provide acceptable levels of information assurance.

e. The NSTISSC will promote the development and adoption of both national and international information assurance standards critical to the protection of national security systems and information and develop a strategy for doing so.

f. The NSTISSC will pursue a strategy for increasing knowledge of the threat to information and systems at the unclassified level; describe associated risks and vulnerabilities; and publicize incidents that reveal real-world attack and vulnerability scenarios. Dissemination of this strategy will be targeted at all operating levels of government departments and agencies.

g. The NSTISSC will sponsor the development of standardized information assurance training for operators and administrators of national security systems and encourage the adoption of similar standardized training for operators and administrators of critical infrastructure systems and networks.

SECTION IV - DEFINTIONS

6. The terms and language used throughout this document reflect standard information systems security (INFOSEC) terminology, as defined in the current version of National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 4009.

a. *National Security Systems*: Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

(1) Involves intelligence activities;

(2) Involves cryptologic activities related to national security;

(3) Involves the command and control of military forces;

(4) Involves equipment that is an integral part of a weapon or weapons system; or,

(5) Is critical to the direct fulfillment of military or intelligence missions, but not including a system that is to be used for routine administrative and business information, such as payroll, finance, logistics, and personnel management information.

b. *National Security Information:* Information that has been determined, pursuant to E.O. 12958, or any predecessor order, to require protection against unauthorized disclosure.

c. *Information Assurance:* Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

d. *Information Systems Security:* The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

e. *Availability:* Timely, reliable access to data and information services for authorized users.

f. *Integrity:* Quality of an Information System (IS) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms and the consistency of the data structures and occurrence of the stored data. Note that, in formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

g. *Authentication:* Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

h. *Confidentiality:* Assurance that information is not disclosed to unauthorized persons, processes or devices.

i. *Non-repudiation:* Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

(b)(3)-P.L. 86-36

DISTRIBUTION:

(b)(3)-P.L. 86-36