NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND

NSA/CSS. REG. 90-6*
DATE: 31 May 199

NSA/CSS REGULATION

NSA/CSS TECHNICAL SECURITY PROGRAM (U)

SECTION I - REFERENCES

1. (U) References

a. (U) Title 10, United States Code, Section 2315

b. (U) DoD Directive C-5200.19, Control of Compromising Emanations, dated 16 May 1995

c. (U) DoD Instruction 5240.5, DoD Technical Surveillance Countermeasures (TSCM) Survey Program, dated 23 May 1984

d. (U) NSA/CSS Regulation 24-2, Counter-intelligence, dated 22 August 1995

SECTION II - TERMINOLOGY

2. (U) For terminology expansion used herein see the attached ANNEX

---

* (U)This Regulation supersedes NSA/CSS Regulation 90-5, TEMPEST Security Program, dated 19 December 1990. OPI: DDI [redacted] C3, 968-7631)

Derived From: NSA/CSSM 123-2, Dated 3 Sep 91
Declassify On: Source Marked "OADR" Date of Source: 3 Sep 91

SECTION III - PURPOSE

3. (U) This regulation establishes the Technical Security Program (TSP) for NSA/CSS. The regulation implements Department of Defense (DoD) and Director, Central Intelligence (DCI), regulatory guidance, establishes policy, assigns responsibilities, and provides for the application of TSCM within NSA/CSS facilities. Also, this regulation replaces NSA/CSS Regulation 90-5, TEMPEST Security Program, dated 19 December 1990, and replaces NSA/CSS Regulation 121-4, NSA/CSS Technical Surveillance Countermeasures Program, dated 15 May 1975. Any pertinent information from those replaced regulations is incorporated in this regulation.

4. (U) The NSA/CSS TSP is established to accomplish the following:

a. (U) Determine the vulnerability to technical exploitation of NSA/CSS facilities and products, equipment, systems and networks that are acquired, designed, or developed by NSA/CSS or used within NSA/CSS facilities to generate, process, communicate, or store national security information or activities/information delineated by reference a;

b. (U) Eliminate or mitigate such vulnerabilities through application of appropriate countermeasures;

c. (U) Support technical security inspection, testing, and evaluation as well as development and application of protective technologies and other countermeasures;

d. (U) Provide for the development and application of techniques, technologies, and instrumentation used to identify technical security vulnerabilities and to prevent, detect, and neutralize adversarial exploitation; and

e. (U) Incorporate traditional TEMPEST and TSCM.

SECTION IV - APPLICABILITY

5. (U) This regulation is applicable to all NSA/CSS elements, plus NSA/CSS field elements and contractors.

SECTION V - POLICY

6. (U) The NSA/CSS TSP established by this regulation will operate according to the following policies:

a. (U) Products, equipment, systems, and networks used to process national security information will be designed, procured, acquired, deployed, and operated in compliance with the applicable technical security standards approved and issued by the Deputy Director for Information Systems Security (DDI).

b. (U) Facilities containing TSP equipment and systems will comply with the requirements prescribed.

c. (U) The DDI, in coordination with the Deputy Director for Support Services (DDS), will direct any Technical Security Evaluation (TSE) of NSA/CSS facilities and NSA/CSS contractor facilities when deemed necessary. NSA/CSS personnel will conduct these evaluations.

d. (C) [redacted]

e. (U) The DDI, in consultation with the Deputy Director for Technology and Systems (DDT) and the Deputy Director for Plans, Policy, and Programs (DDP), will share, as appropriate, techniques, technology, and instrumentation from the NSA/CSS TSP with the U.S. government's national technical security community assisting the U.S. effort to defend against and detect adversarial attacks.

SECTION VI - RESPONSIBILITIES

7. (U) The DDI shall:

a. (U) Act for the Director of NSA and Chief, CSS (DIRNSA/CHCSS), in fulfilling the responsibilities assigned to him by reference b, sections E.4. and 6, and reference c, sections F.2. and 3, except those responsibilities stated below in paragraphs 9.d. and 13;

b. (U) Act as the principal advisor to DIRNSA/CHCSS on matters concerning technical security and provide recommendations on the sufficiency of NSA/CSS programs for technical security;

c. (U) Serve as the NSA/CSS technical security spokesperson to the Intelligence Community and U.S. Government agencies;

d. (U) Serve, in coordination with DDT, the Deputy Director for Operations (DDO), and DDP, as the NSA/CSS technical security spokesperson to all foreign governments having technical security exchanges with NSA/CSS;

e. (U) Develop and recommend to DIRNSA/CHCSS, in coordination with DDP, DDT, DDO, and DDS, technical security plans, policies, objectives, and implementation strategies;

f. (U) Establish appropriate technical security standards, techniques, performance specifications, technical requirements, and life-cycle technical security requirements (e.g., shipping handling, maintenance, etc.) for both cryptographic and noncryptographic equipment and systems for use at NSA/CSS and NSA/CSS contractor facilities;

g. (U) Establish, in concert with DDS, technical security standards for NSA/CSS and NSA/CSS contractor facilities in compliance with standards promulgated by the DCI or other appropriate higher authorities;

h. (U) Evaluate information systems security (INFOSEC) equipment and systems during their design, development, and operational use ensuring that technical security requirements are achieved;

i. (U) Conduct or request DDT support to perform research, development, test, and evaluation on equipment and system tamper detection and integrated circuit protection techniques;

j. (U) Implement equipment and system tamper detection and integrated circuit protection techniques for INFOSEC products and equipment;

k. (U) Identify, plan, prioritize, and conduct, in coordination with DDS, technical security evaluations of NSA/CSS headquarters, field, and contractor facilities or arrange for these evaluations to occur. As necessary, DDS will orchestrate the prioritization of specific evaluations using site specific vulnerability, threat, and countermeasure information;

l. (U) Provide DDS with the findings of the technical security evaluations and inspections for those facilities under NSA/CSS security cognizance prior to the release of those findings to the evaluated facility;

m. (U) Resolve requests for technical security waivers (see SECTION VII of this regulation);

n. (U) Provide appropriate representation and leadership to the national technical security fora;

o. (U) Develop, evaluate, and apply technical security facility countermeasures in coordination with the DDS and other affected parties.

p. (U) Provide technical security advice and assistance to Service Cryptologic Elements (SCE), as requested;

q. (U) Identify to DDS technical security training requirements;

r. (U) Conduct or request support of DDT to perform research, development, test, and evaluation in support of NSA/CSS technical security;

s. (U) Arrange for and/or provide support in technical security to other DoD components or other U.S. Government departments and agencies;

t. (U) Report to DDS all known or suspected penetrations of NSA/CSS facilities, products, equipment, systems, and networks for appropriate counterintelligence investigation;

u. (U) Provide technical security advice and assistance to F6, upon request from the F6 Cognizant Security Authority (CSA). The F6 CSA will ensure that F6 technical security needs and countermeasures are satisfied through close coordination with a DDI spokesperson;

v. (U) Establish a mechanism for the expeditious handling, in concert with DDS, of technical security emergencies affecting facilities under NSA/CSS security cognizance; and

w. (U) As required, the DDI shall periodically convene a forum, consisting of representatives from Key Components, for discussion of matters relative to NSA/CSS's Technical Security Program.

8. (U) The DDS shall:

a. (U) Include technical security as part of the NSA/CSS security program and implement physical and personnel security policies consistent with the NSA/CSS TSP;

b. (U) Include technical security in the NSA/CSS Security Awareness Program;

c. (U) Recommend to the DDI, NSA/CSS facilities and NSA/CSS contractor facilities to undergo a TSE;

d. (U) Advise DDI on counterintelligence issues effecting the TSP;

e. (U) Facilitate any TSE by arranging for the support and cooperation of key component and field activity special security officers;

f. (U) Coordinate with the DDI before the construction or renovation of NSA/CSS facilities to ensure identification of technical security concerns;

g. (U) Include technical security requirements identified by DDI in construction plans for new or refurbished buildings;

h. (U) Provide the necessary technical security training; and

i. (U) Conduct counterintelligence investigations of known or suspected technical penetrations of NSA/CSS facilities, products, equipment, systems, and networks in accordance with reference d.

9. (U) The DDT shall:

a. (U) Conduct research, development, test and evaluation (RDT&E) to support NSA/CSS technical security objectives and respond to tasking from the DDI in these areas;

b. (U) Evaluate and test new technologies as adversarial methodologies are identified and recommend to the DDI specific methods to counter these attacks;

c. (S) [redacted]

d. (U) Conduct RDT&E on equipment and system tamper protection and integrated circuit protection techniques and respond to tasking from DDI in these areas; and

e. (U) Purchase, lease, install, and operate only those equipment and systems that meet the technical security requirements.

10. (U) The DDP shall ensure items entered into inventory under DDP cognizance meet established TSP requirements.

11. (U) The DDO shall respond to SIGINT requirements from DDI and provide DDI any information derived from SIGINT about foreign exploitation of U.S. facilities, products, equipment, networks, or systems.

12. (U) The Chiefs of Key Components and Field Activities shall:

a. (U) Establish procedures for implementing the requirements of the TSP;

b. (U) Ensure compliance with applicable TSP requirements in the acquisition, development, operation, maintenance, and protection of products, equipment, systems, networks, and facilities;

c. (U) Report possible technical security weaknesses, problems, or suspicious circumstances to DDI and DDS spokespersons;

d. (U) Accommodate technical security evaluation efforts and arrange for DDI technical security support; and

e. (U) Designate a Key Component or Field Activity technical security coordinator.

13. (U) The Inspector General shall, because of the significant cost implications and in response to U.S. National and DoD requirements, perform oversight of the application of TSCM and make the application of technical security at NSA/CSS an item of recurring interest.

14. (U) All NSA/CSS personnel responsible for the design, development, acquisition, deployment, and operation of equipment and systems that will be used to process national security information or responsible for the facilities that contain such equipment shall comply with applicable technical security requirements issued by the DDI.

SECTION VII - WAIVERS

15. (U) If the requirements of the TSP cannot be met, waivers are required. Requests for technical security waivers must be submitted by the Key Component or Field Activity technical security coordinator, through the Chief of the Key Component or Field Activity, to the DDI designee. Waiver requests for facilties under NSA/CSS security cognizance shall be evaluated by the DDI designee, in coordination with the DDS. If a satisfactory solution to the problem cannot be achieved, the waiver request will be forwarded to the DDI for resolution. If the waiver is granted, the DDI will conduct follow-up inspections to ensure the conditions of the waiver are being followed.

THOMAS J. McDERMOTT
Deputy Director
for
Information Systems Security

Encl:
a/s

DISTRIBUTION III
Plus: C3 (30 stock copies)
F92 (VRD)
N5P1

ANNEX - TERMINOLOGY

The following terms used in this document are not found in NSTISSI No. 4009, National Information Systems Security Glossary.

1. (U) Technical Security: The discovery, elimination, and mitigation of security vulnerabilities that can be exploited by technical means. It includes all facets of security that involve the detection and/or neutralization of technical collection threats or the application of security technology; the traditional fields of TEMPEST and technical surveillance countermeasures (TSCM); and extends to new techniques, technology, and instrumentation that may allow exploitation of security vulnerabilities by technical means.

2. (U) Technical Security Evaluation (TSE): An evaluation of all factors related to potential vulnerabilities of technical penetration of a facility, system, network, product, or equipment. Typical considerations include security against acoustical, optical, audio frequency, radio frequency, and other methods of penetration as well as adequacy of electronic protection. A TSE includes TSCM, TEMPEST, and TEAPOT considerations.

3. (C) [redacted]

Derived From: NSA/CSSM 123-2
Dated 3 Sep 91
Declassify On: Source Marked "OADR"
Date of Source: 3 Sep 91

ANNEX to
NSA/CSS Reg. No. 90-6

4. (U) TEAPOT: A short name referring to the investigation, study, and control of intentional compromising emanations (i.e., those that are hostilely induced or provoked) from telecommunications and automated information systems equipment.

5. (U) NSA/CSS Facilities: All NSA headquarters facilities, field activities, and contractor facilities under security cognizance of NSA/CSS.