NSTISSP No. 5
August 30, 1993

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

NATIONAL POLICY

FOR

INCIDENT RESPONSE AND

VULNERABILITY REPORTING

FOR NATIONAL SECURITY SYSTEMS

~~FOR OFFICIAL USE ONLY~~

NSTISSC
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CHAIRMAN

August 30, 1993

FOREWORD

In recent years, numerous attacks have been mounted against U.S. Government telecommunications and information systems. The increasing numbers of these attacks, and the use of telecommunications and information systems networks that crossed agency lines, made it apparent that information concerning these events needed to be disseminated among U.S. Government organizations.

This policy establishes the requirement for U.S. Government departments and agencies involved with national security systems, as defined in National Security Directive 42, dated July 5 1990, to collaborate and cooperate with other appropriate organizations in the sharing of incident, vulnerability, threat, and countermeasures information concerning those systems.

/s/

MR. EMMETT PAIGE,

NATIONAL POLICY FOR INCIDENT RESPONSE AND VULNERABILITY REPORTING FOR NATIONAL SECURITY SYSTEMS

SECTION I - POLICY

1. Recent events involving the use of international telecommunications and computer systems to attempt to exploit and disrupt national security systems, as defined in National Security Directive 42, dated July 5, 1990, clearly underscore the need for an organized and fully supported capability to deal with such incidents. Accordingly, U.S. Government departments and agencies involved with national security systems shall collaborate and coordinate efforts to:

a. contain and minimize the impact of security incidents on national security systems, and

b. eliminate or minimize vulnerabilities among national security systems.

SECTION II - SCOPE AND APPLICABILITY

2. This policy focuses on security incidents and vulnerabilities that threaten national security systems.

3. This policy is applicable to U.S. Government departments, agencies, and their contractors that acquire, develop, use, maintain, or dispose of national security systems.

SECTION III - RESPONSIBILITIES

4. Heads of U.S. Government departments and agencies involved with national security systems shall implement this policy consistent with established procedures.

NSTISSC
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CHAIRMAN

August 30, 1993

FOREWORD

In recent years, numerous attacks have been mounted against U.S. Government telecommunications and information systems. The increasing numbers of these attacks, and the use of telecommunications and information systems networks that crossed agency lines, made it apparent that information concerning these events needed to be disseminated among U.S. Government organizations.

This policy establishes the requirement for U.S. Government departments and agencies involved with national security systems, as defined in National Security Directive 42, dated July 5 1990, to collaborate and cooperate with other appropriate organizations in the sharing of incident, vulnerability, threat, and countermeasures information concerning those systems.

Mr. Emmett Paige, JR.

(b) (6)