(S) National Security Agency/Central Security Service (NSA/CSS) and U.S. Strategic Command Joint Functional Component Command – Network Warfare (JFCC-NW)

National Initiative Protection Program – Sentry Eagle

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20310524

(S) NSA/CSS/JFCC-NW National Initiative Brief Sheet

1. (S//NF) You are being indoctrinated on SENTRY EAGLE, the NSA/CSS and JFCC-NW's compartmented program protecting the highest and most sensitive level of information related to NSA/CSS's and JFCC-NW's support to the U.S. Government's efforts to protect America's cyberspace. America's cyberspace is the combination of U.S. National Security Systems, Military Systems, Intelligence Systems, Federal Government Systems, Critical Infrastructure Systems and all other U.S. systems (private industry, academia and private citizen.)

2. (S//NF) NSA/CSS's effort to protect America's cyberspace encompasses the combination of all abilities to detect nation and non-nation attacks on U.S. cyberspace via active and passive SIGINT and Information Assurance means. JFCC-NW's effort to protect America's cyberspace encompasses the efforts to plan, synchronize, and when tasked, attack an adversary's cyber space via Computer Network Attack. The combination of these two efforts constitutes NSA/CSS's and JFCC-NW's Core Computer Network Operations (CNO) Secrets.

3. (TS//SI//NF) In order for NSA/CSS and JFCC-NW to accomplish, along with other U.S. and foreign government agencies/elements, the protection of America's cyberspace, NSA/JFCC-NW must combine the full capabilities of authorized Computer Network Operations capabilities (SIGINT, Computer Network Exploitation (CNE); Information Assurance, Computer Network Defense (CND), and Network Warfare, Computer Network Attack (CNA)) and all supporting activities.

4. (TS//SI//NF) SENTRY EAGLE and its subordinate programs protect the combined facts related to NSA/CSS and JFCC-NW's abilities to conduct CNO operations. It encompasses the most sensitive aspects of NSA/CSS's: relationships with industry (U.S. and foreign) and the U.S. Information Operations/CNO community; ability to exploit enciphered communications; ability to conduct CNE; ability to conduct CND; and, relationships with Human Intelligence (HUMINT) Agencies.

5. (TS//SI//NF) These NSA/CSS and JFCC-NW Core CNO Secrets are being provided to you based upon your "need to know" as determined by the Director, NSA/Chief, Central Security Service and Commander, JFCC-NW. While many of the facts in this briefing are contained in separate NSA/CSS Exceptionally Controlled Information (ECIs) or DOD Special Access Programs (SAPs) structures, no other program combines the totality of all these facts into one overarching program. The facts contained in this program constitute a combination of the greatest number of highly sensitive facts related to NSA/CSS's overall cryptologic mission. As such, depending upon

your mission need-to-know or management position, you may be read on for one, a combination of two or more, or all aspects of SENTRY EAGLE.

6. (TS//SI//NF) Individuals briefed into SENTRY EAGLE may not share information regarding this program with those not read into this program, or with foreign nationals, including those with whom NSA/CSS has Second and Third Party relationships. Depending upon a specific fact, you may share such a fact with foreign partners as noted on the SENTRY EAGLE or subordinate classification guides as paragraph marked or within specific NSA/CSS SAP or ECI channels. Under no circumstances will you share the totality of SENTRY EAGLE nor facts that are marked NOFORN.

7. (S) SENTRY EAGLE material must be protected within this compartment and discussed only with cleared personnel on a need-to-know basis. Disclosure of SENTRY EAGLE information to non-indoctrinated personnel may result in disciplinary action to include criminal prosecution. When sharing SENTRY EAGLE compartmented information, it will be protected with PKI when transmitted via electronic means or with sealed, by name envelopes when transmitted via hard copy.

(U) SENTRY EAGLE DATA SHEET

(U//FOUO) COVERNAME: SENTRY EAGLE

(U//FOUO) TRIGRAPH: SEE

(U//FOUO) CONTROL AUTHORITY CONTACT INFORMATION:

Name: [redacted]
Org: [redacted]
Phone #: [redacted]
E-mail: [redacted]

Name: [redacted]
Org: [redacted]
Phone #: [redacted]
E-mail: [redacted]

(U) INFORMATION REQUIRING SENTRY EAGLE PROTECTION:

(TS//SI//NF) Details related to the combination of NSA/CSS's and JFCC-NW's abilities to conduct CNO in the defense of America's cyberspace.

(U) VALUE OF SEE:

(TS//SI//NF) Protecting sensitive NSA/CSS industrial and human intelligence relationships; SIGINT exploitation of adversary computers and computer networks and infrastructure and their use of encipherment; Information Assurance defense of U.S. Government National Security Systems; and, JFCC-NW's Computer Network Attack mission capabilities.

(U) JUSTIFICATION FOR SENTRY EAGLE PROTECTION:

(TS//SI//NF) Unauthorized disclosure of NSA/CSS relationships with industry (U.S. and foreign) and the U.S. Information Operations/CNO community; ability to exploit enciphered communications; ability to conduct CNE; ability to conduct CND; and, relationships with Human Intelligence (HUMINT) Agencies will cause exceptionally grave damage to U.S. national security. The loss of this information could critically compromise highly sensitive cryptologic U.S. and foreign relationships, multi-year past and future NSA investments, and the ability to exploit foreign adversary cyberspace while protecting U.S cyberspace.

(U) LINKAGE TO OTHER NSA/CSS and JFCC-NW PROGRAMS (ECI or SAP):

(C) This overarching compartmented program is related to the following ECIs (list all the ECIs – SPARECHANGE, WHIPGENIE, AUNTIE, AMBULANT, OPALESCE, REVELRY, REFRACTOR) and SAPs (list all the SAPs – by name only).

(C) SENTRY EAGLE is an umbrella ECI program that includes facts currently contained in other NSA/CSS ECIs and separate SENTRY EAGLE ECI facts.

(C) SENTRY EAGLE contains sub-compartments: SENTRY HAWK, SENTRY FALCON, SENTRY OSPREY, SENTRY RAVEN, SENTRY CONDOR, AND SENTRY OWL.

(U) WILL SENTRY EAGLE BE SHARED WITH FOREIGN PARTIES?

(S//SI//NF) The entirety of SENTRY EAGLE will not be shared with any foreign parties. However, subcomponents of SENTRY EAGLE, constituting various facts already shared with 2nd or 3rd parties, may be shared, but only within existing NSA/CSS ECIs. See specific ECI Security Officers for more information on sharing with foreign partners.

(S//NF) What follows is a listing of NSA/CSS and JFCC-NW generalized facts related to sensitive intelligence and defense or network warfare methods, relationships and activities that are currently protected as noted. Many of these facts, to include detailed information, are contained in separate special access programs under NSA/CSS auspices – many under Exceptionally Controlled Information (ECIs) or Special Access Programs (SAPs).

(S) The protection of Intelligence sources, methods and activities relate to the following: Source – Person, place or thing from which intelligence is gathered; Method – means by which collection, processing, and dissemination takes place; Activity – intelligence operation that may employ one or more source or method and the degree of success for said operation.

(S//NF) Depending upon your mission need-to-know, you will be read on for one or more of these generalized fact sets. Specific detailed facts for a generalized fact will remain within one or more ECIs as noted.

(U) Facts, as color coded, are as follows:

a. (U) **Green color**: Unclassified facts that may be released to the public at the unclassified level. Only NSA/CSS or JFCC-NW Public Affairs officers may release this information.
b. (U//FOUO) **Blue color**: Unclassified but for Official Use Only (FOUO) facts that may be released by any NSA/CSS or JFCC-NW government official to another U.S. Government, U.S. Industry, U.S. Academic or selected foreign governments, as authorized.
c. (U//FOUO) **Red color**: Confidential, Secret or Top Secret, to include Special Compartmented Information (SCI), that may be released by any NSA/CSS and JFCC-NW government official to another properly cleared and indoctrinated U.S. Government official or as authorized to a foreign government on need to know basis.
d. (S//NF) **Black color**: Top Secret, NATIONAL INITIATIVE/SENTRY EAGLE program information that MAY NOT BE RELEASED OUTSIDE OF NSA/CSS except to a limited number of selected U.S. Government officials and ONLY WITH THE APPROVAL OF DIRNSA/CHCSS/CDR, JFCC-NW OR THE NATIONAL INITIATIVE PROGRAM SECURITY OFFICER. These facts, in part or as a whole, constitute many of NSA/CSS's and JFCC-NW's most highly sensitive cryptologic or network warfare facts related to intelligence sources, methods, and activities and relationships; or CNA operational capabilities, thus necessitating extraordinary protection.

(U) NSA/CSS and its Relationships with Industry within the National Imitative – ECI Sentry Owl - SOL

(U) Fact that NSA/CSS must keep abreast of current trends and technology related to communications and information technology.
(U) Fact that NSA/CSS works with foreign partners as a part of its cryptologic missions.

(U//FOUO) Fact that NSA/CSS works with U.S. industry in the conduct of its cryptologic missions.
(U//FOUO) Fact the NSA/CSS works with U.S. industry as technical advisors regarding cryptologic products.

(TS//SI) Fact that NSA/CSS conducts SIGINT enabling programs and related operations with U.S. industry.
(TS//SI) Fact that NSA/CSS conducts SIGINT enabling programs and related operations with U.S. HUMINT Agencies and other U.S. government elements.
(TS//SI//NF) Fact that NSA/CSS has Foreign Intelligence Surveillance Act (FISA) operations with U.S. commercial industry elements.
(TS//SI) Fact that NSA/CSS conducts SIGINT enabling programs and related operations with foreign partners.

(TS//SI//ECI SOL) Fact that NSA/CSS works with and has contractual relationships with specific named U.S. commercial entities (A/B/C) to conduct SIGINT enabling programs and operations.
(TS//SI// ECI SOL) Fact that NSA/CSS works with specific named U.S. commercial entities (A/B/C) and operational details (devices/products) to make them exploitable for SIGINT.
(TS//SI// ECI SOL) Fact that NSA/CSS works with specific foreign partners (X/Y/Z) and foreign commercial industry entities (M/N/O) and operational details (devices/products) to make them exploitable for SIGINT.
(TS//SI//ECI SOL) Facts related to NSA personnel (under cover), operational meetings, specific operations, specific technology, specific locations and covert communications related to SIGINT enabling with specific commercial entities (A/B/C).
(TS//SI//ECI SOL) Facts related to NSA/CSS working with U.S. commercial entities on the acquisition of communications (content and metadata) provided by the U.S. service provider to worldwide customers; communications transiting the U.S.; or access to international communications (cable, satellite, etc.) mediums provided by the U.S. entity.
(TS//SI// ECI SOL) Facts that identify a U.S. or foreign commercial platform conducting SIGINT operations, or human asset cooperating with NSA/CSS.

(U) NSA/CSS and its Relationships to Information Operations/Computer Network Operations with the National Initiative – ECI Sentry Condor - SCR.

(U) Fact that NSA/CSS provides cryptologic support to Information Operations (IO).
(U) Fact that NSA/CSS provides SIGINT and Computer Network Defense (CND) information in support of Computer Network Attack (CNA).

(U//FOUO) Fact that NSA/CSS provides technical SIGINT and Information Assurance data/information in support of CNO

(TS//SI) Fact that NSA/CSS provides SIGINT that supports the planning, deployment/emplacement and employment of CNA combat capabilities
(TS//SI) Fact that NSA/CSS hosts (specific DOD named units and organizations) CNA activities within its SIGINT CNE structure.

(TS//SI//NF//ECI SCR) Fact that NSA/CSS provides specific target related technical and operational material (identification/recognition), tools and techniques that allows the employment of U.S. national and tactical specific computer network attack mechanisms.

(U) NSA/CSS and Exploitation of Enciphered Communications with the National Imitative – ECI Sentry Raven - SRN

(U) Fact that NSA/CSS exploits foreign ciphers.

(U//FOUO) Fact that NSA/CSS works with the UK/CAN/AUS/NZ in the exploitation of foreign ciphers.

(TS//SI) Intelligence derived from the exploitation of foreign ciphers without revealing the underlying foreign cipher (manual or machine) or techniques used to exploit.

(TS//SI//ECI SRN) Facts that reveal specific cryptographic weakness or cryptanalytic methods/means/techniques used to achieve success against a foreign cipher.
(TS//SI//ECI SRN) Facts related to Super Computers/Special Purpose cryptanalytic hardware, software and specific programmatic funding resources used to achieve success against foreign ciphers.
(TS//SI// ECI SRN) Fact that NSA/CSS works with specific U.S. commercial entities (A/B/C) to modify U.S. manufactured encryption systems to make them exploitable for SIGINT.
(TS//SI//NF//ECI SRN) Fact that NSA/CSS is investing hundreds of millions of dollars in high-powered and special purpose computer systems to attack (specifically X/Y/Z) commercial encryption.

(U) NSA/CSS and Computer Network Exploitation with the National Initiative – ECI Sentry Hawk - SHK

(U) Fact the NSA/CSS conducts Computer Network Exploitation (CNE)
(U) Fact that NSA/CSS works with the CIA and FBI.

(U//FOUO) Fact that NSA/CSS works with CIA and FBI on SIGINT related missions.

(S//SI) Fact that NSA/CSS works with CIA and FBI related to "close access or remote access" CNE operations.
(S//SI) Fact that NSA/CSS conducts SIGINT operations against computers, computer peripherals, computer-controlled devices, computer networks or facilities that house them, using publicly available access (e.g. Public Switched Networks, Internet, etc.).
(TS//SI) Facts related to adversary vulnerabilities to CNA.
(TS//SI) Facts related to adversary CNA/CNE planning or operations.*

(TS//SI//ECI SHK) Fact that NSA/CSS is attempting to exploit or has succeeded in exploiting a specific vulnerability (e.g. firewall, operating system, software application etc.), a specific entity or facility within a target's IT/computer structure.
(TS//SI// ECI SHK) Facts related to the exact timing, location, participants, off-net or on-net operations (including cover/covert presence on the internet), CNE command, control and data exfiltration tools/capabilities and locations, used to exploit or maintain intrusive access to a target's IT/computer structure.
(TS//SI//ECI SHK) Fact that NSA/CSS works with U.S. and foreign commercial entities (A/B/C) in the conduct of CNE.
(TS//SI//ECI SHK) Facts related to the description of U.S. hardware or software implant and location (specific organization and Internet Protocol Device/Address) of such on a target's IT/communications system.
(TS//SI//ECI SHK) Facts related to NSA/CSS's access to non-U.S. worldwide cable/fiber optic structures regardless of platform access or agreements with foreign entities.

* (TS//SI) (Note: All attempts will be made to protect the "source" of the CNA/CNE information lest an adversary determine how NSA acquired the CNA/CNE planning and operations. In all cases, maximum protection will be granted to the SIGINT "method" and "activity" used to acquire the CNA/CNE information).

(U) NSA/CSS and Computer Network Defense with the National Imitative – ECI Sentry Falcon - SFN

(U) The fact that NSA/CSS conducts Computer Network Defense (CND)
(U) Facts related to general, open source reporting on types of generic vulnerabilities (viruses, trojan horses, etc.)

(U//FOUO) Facts related to NSA/CSS's deployment of CND structures to detect and report on anomalous activities.
(U//FOUO) General facts related to NSA/CSS's Joint COMSEC Monitoring Activities (JCMA), Red Team and Blue Team.
(U//FOUO) Facts related to U.S. victim vulnerabilities and victim exploitation when uncovered via Bluesash.

(C/NF) Facts related to NSA/CSS JCMA results as provided to a supported command*.
(S) Facts related to adversary CNE and CNA capabilities, intentions and activities (without attribution to intelligence sources or methods**)
(S) Facts related to NSA/CSS's deployment of CND structures (e.g. Bluesash) to detect hostile (state or non-state sponsored) CNE activities at U.S. NIPRNET gateways.
(S) CND response action operations.
(S) Facts related to NSA/CSS's Joint COMSEC Monitoring Activities (JCMA), Red Team, Blue Team results***.
(S//SI) Facts related to adversary CNE and CNA activity attribution. **
(S//SI) Facts related to U.S. victim vulnerabilities and victim exploitation when uncovered via SIGINT sources and methods.
(TS//SI) Facts related to U.S. victim vulnerabilities and victim exploitation. **

(TS//NF// ECI SFN) Facts related to NSA/CSS activities to determine intruder attribution including sensitive counter-intelligence investigations and sensitive honey-pot, watermarking, data-tagging activities.
(TS//NF//ECI SFN) Facts related to NSA/CSS specific operations to deceive network users.
(TS//NF//ECI SFN) Facts related to NSA/CSS specific activities to redirect network data.

*(C) Classified at a minimum C//NF. May be classified higher based upon results.

**(S) Note: The only way to accomplish this outside of SCI, but still classified, channels may necessitate the use of a U.S. Government (e.g. Department of Homeland Security) "cut-out" to transmit such information to U.S. Government, State, Local and Tribal entities, as well as foreign governments. The preference will be to use a non-U.S. Intelligence Community entity.

*** (S) Results may be Secret NOFORN.

(U) NSA/CSS and its Relationship with Human Intelligence (HUMINT) Agencies with the National Initiative – ECI Sentry Osprey - SOY

(U) Fact that NSA/CSS works with the Central Intelligence Agency (CIA) and the Defense Human Intelligence via the National Clandestine Service (NCS).

(U//FOUO) Fact the NSA/CSS works with the NCS to conduct SIGINT operations.

(TS//SI//NF) Fact that NSA/CSS works with the NCS for the collection of high priority target internal foreign communications.
(TS//SI) Fact that NSA/CSS employs its own HUMINT assets (Target Exploitation – TAREX) to support SIGINT operations.

(TS//SI//NF//ECI SOY) Facts related to NSA/CSS targets/target countries that employ NCS capabilities.
(TS//SI//NF//ECI SOY) Facts related to the identity of NCS human assets/agents (covert or under cover), specific targets/target countries, specific locations/sites (cities/IT site) and specific operations and techniques (equipments/supply chain or other) used to exploit targets.