(U) CLASSIFICATION GUIDE TITLE/NUMBER: **Computer Network Exploitation (CNE) Classification Guide / 2-59**

(U) PUBLICATION DATE: 1 March 2010

(U) OFFICE OF ORIGIN: Tailored Access Operations (TAO)/S32

(U) POC: TAO Classification Advisory Officer

(U) PHONE: 961-6794s

(U//FOUO) ORIGINAL CLASSIFICATION AUTHORITY: SIGINT Deputy Chief of Staff for Operations and Support, [redacted]

Description of Information	Classification/Markings	Reason	Declass	Remarks
A. (U) GENERAL				
1. (U) The fact that NSA/CSS or TAO performs computer network exploitation (CNE)	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
2. (S//REL) The fact that NSA/CSS or TAO, as part of CNE operations, performs remote subversion	SECRET//REL TO USA, FVEY	Sec 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level and/or require compartmentation. (U) Foreign releasability decisions on specific details relating to remote subversion are handled on a case-by-case basis. Contact TAO CAO for further guidance.
3. (S//SI//REL) Identification of specific remote subversion methods used by NSA/CSS or TAO, to include: - Endpoint access, exploitation, or operations - On-net access, exploitation, or operations - Software implant access, exploitation, or operations - Accessing or exploiting data at rest	SECRET//SI//REL TO USA, FVEY	Sec 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level and/or require compartmentation. (U) Foreign releasability decisions on specific details relating to remote subversion are handled on a case-by-case basis. Contact TAO CAO for further guidance.
4. (S//SI//REL) The fact that NSA/CSS or TAO, as part of CNE operations, performs physical subversion, to include:	SECRET//SI//REL TO USA, FVEY	Sec 1.4 (c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification and

- Close access enabling, exploitation, or operations - Off-net enabling, exploitation, or operations - Supply chain enabling, exploitation, or intervention operations - Hardware implant enabling, exploitation, or operations				require ECI protection. (U) Foreign releasability decisions on specific details relating to physical subversion are handled on a case-by-case basis. Contact TAO CAO for further guidance.
5. (U) The association of any specific ECI name or trigraph, with NSA/CSS, ECI, SIGINT, or intelligence	UNCLASSIFIED//FOR OFFICIAL USE ONLY	FOIA 3	N/A	
6. (U) The association of a specific TAO ECI name or trigraph with CNE and/or TAO	CONFIDENTIAL//REL TO USA, FVEY	Sec. 1.4(c)	N/A	
7. (U) The fact that a specific individual is cleared for a specific TAO ECI, when there is no association between the ECI and TAO	UNCLASSIFIED//FOR OFFICIAL USE ONLY			(U) If the details of the association reveal the fact that the ECI is TAO's, then it would be CONFIDENTIAL//REL TO USA, FVEY, in accordance with entry 5.
8. (U) The fact that NSA/CSS or TAO conducts CNE for foreign intelligence collection.	UNCLASSIFIED	N/A	N/A	
9. (U) The fact that NSA/CSS or TAO, as part of CNE operations, performs CNE to support U.S. Government CNA efforts	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
10. (U) The fact that NSA/CSS or TAO, as part of CNE operations, trains, equips, and organizes the U.S. Cryptologic System to support the CNE, CNA, and CND requirements needs of its customers	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
11. (U) The fact that NSA/CSS or TAO, as part of CNE operations, provides CNO-related military targeting support	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
12. (U) The fact that NSA/CSS or TAO, as part of CNE operations, provides intelligence gain/loss assessments in response to Combatant Commander (COCOM) CNO targeting	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
13. (U) The fact that NSA/CSS or TAO, as part of CNE operations, develops and supports analytic modeling and simulation techniques to support CNE/CNA efforts	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.

14. (U) The fact that NSA/CSS or TAO, as part of CNE operations, targets, collects and processes computers, computer networks and computer-to-computer (C2C) communications without reference to a specific operation, activity or target	UNCLASSIFIED	N/A	N/A	(U) Details indicating specific targets, level of success or capabilities remain classified.
15. (S//SI//REL) The fact that NSA or TAO, as part of CNE operations, targets, collects and processes specific computer protocols (such as email, instant messaging, file transfer protocols)	SECRET//SI//REL TO USA, FVEY	Sec 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level to TOP SECRET. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN).
16. (S//SI//REL) The fact that NSA/CSS or TAO, as part of CNE operations, remotely introduces code into target computer networks to facilitate foreign intelligence collection	SECRET//SI//REL TO USA, FVEY	Sec 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level to TOP SECRET. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN).
17. (TS//SI//REL) The fact that NSA/CSS or TAO, as part of CNE operations, conducts off-net field operations to develop, deploy, exploit, or maintain intrusive access, without further detail	TOP SECRET//SI//REL TO USA, FVEY	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN).
18. (S//SI//REL) The fact that NSA/CSS or TAO, as part of CNE operations, conducts off-net activities at specified locations other than NSA/CSS facilities	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may also be protected by an ECI. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
19. (U) TAO project names, in association with CNE or TAO, with no amplifying details	UNCLASSIFIED//FOR OFFICIAL USE ONLY	FOIA (3)	N/A	
B. (U) PARTNERING/COLLABORATION				
20. (C//REL) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with Second Party Partners to conduct CNE activities	CONFIDENTIAL//REL TO USA, FVEY	Sec 1.4(c, d)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level. (U) Details may also be protected by one or more

				ECIs.
21. (C//REL) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with specific Second Party partners on specific ECIs	CONFIDENTIAL//REL TO USA, FVEY See remarks for foreign releasability.			(U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
22. (C//REL) Details of the CNE collaboration between NSA/CSS or TAO and Second Party partners	SECRET//SI at a minimum See remarks for foreign releasability.			(U) Details indicating specific targets, level of success or capabilities may raise the classification level to TOP SECRET//SI. (U) Details may also be protected by one or more ECIs. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
23. (S//REL) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with unspecified Third Party Partners in support and conduct of CNE activities	SECRET//REL TO USA, FVEY	Sec 1.4(c, d)	*25 years	(U) Details may also be protected by an ECI. Contact TAO CAO for further guidance.
24. (S//REL) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with specified Third Party Partners in support and conduct of CNE activities	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c, d)	*25 years	(U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance. (U) Details may also be protected by an ECI. Contact TAO CAO for further guidance.
25. (U//FOUO) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with a specific US Government/IC entity	UNCLASSIFIED//FOR OFFICIAL USE ONLY	FOIA (3)	N/A	(U) Details indicating specific targets, level of success or capabilities may raise the classification level. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN).
26. (C//REL) The fact that NSA/CSS or TAO, as part of CNE operations, collaborates with a specific US Government/IC entity on a specific ECI	CONFIDENTIAL//REL TO USA, FVEY	Sec. 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN).

C. (U) TOOLS AND TECHNIQUES				
27. (U) The existence of CNE tools, with no further details/context	UNCLASSIFIED	N/A	N/A	
28. (U) Cover names of CNE tools, with no details/context	UNCLASSIFIED	N/A	N/A	
29. (S//SI//REL) When associated with remote subversion, details/descriptions concerning CNE tools, to include: - Specific type (i.e. hardware/software, etc.) - Purpose - Capabilities - Concealment Techniques - Electronic signatures - Combination(s) of the above	SECRET//SI at a minimum See remarks for foreign releasability.	Sec. 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level to TOP SECRET. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN). (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
30. (S//SI//REL) When associated with physical subversion, details/descriptions concerning CNE tools, to include: - Specific type (i.e. hardware/software, etc.) - Purpose- - Capabilities - Concealment Techniques - Electronic signatures - Combination(s) of the above	TOP SECRET//SI See remarks for foreign releasability	Sec 1.4(c)	*25 years	(U) Details indicating specific targets, level of success or capabilities may raise the classification level to TOP SECRET. (U) Details may also be protected by one or more ECIs and/or a different level of foreign releasability (including NOFORN). (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
31. (U//FOUO) Technical details concerning specific software vulnerabilities, **when publicly known**, and that are exploited for CNE activities	UNCLASSIFIED//FOR OFFICIAL USE ONLY	FOIA (3)	N/A	
32. (S//SI//REL) Technical details concerning specific software vulnerabilities, **when not publicly known**, and that are exploited for CNE activities	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may be protected as NOFORN on a case-by-case basis. (U) Some tools may be protected under an ECI and/or additional handling caveats. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.

D. (U) OPERATIONS and TARGETING				
33. (U) The fact that NSA/CSS or TAO, as part of CNE operations, targets a specific country or international organization	SECRET//SI//REL TO USA, FVEY at a minimum	Sec. 1.4 (c)	*25 years	(U) Details may also be protected by a different level of foreign releasability (including NOFORN). (U) Contact TAO CAO for further guidance on levels of success as well as for more specific targeting details such as individual(s), specific government entity(ies), etc.
34. (S//SI//REL) Association of cover names for off-net operations (i.e., physical subversion activities) with amplifying details (e.g., specific electronic components, systems, their host facilities, etc)	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more ECIs. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
35. (S//REL) Association of cover names for on-net operations (i.e., remote subversion activities) with amplifying details (e.g., specific electronic components, systems, their host facilities, etc)	SECRET//SI at a minimum See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more ECIs. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
36. (S//SI//REL) **Individual** details of CNE activities, such as: - Target information including intended target network and/or device - Vulnerability being targeted - Target infrastructure	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4 (c)	*25 years	(U) Details may also be protected by one or more ECIs. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
37. (TS//SI//REL) The fact that NSA/CSS or TAO, as part of CNE operations, is attempting to exploit or has succeeded in exploiting a specific vulnerability (e.g., in a firewall, operating system, software application, etc.), and a specific entity or facility within a target's IT/computer structure	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more ECI. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
38. (S//SI//REL) Facts related to the description of U.S. hardware or software implants and location (e.g., specific organization and Internet Protocol Device/Address, etc.) on a target's IT/communications system	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more ECI. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
39. (S//SI//REL) Facts related to the exact timing, location,	TOP SECRET//SI at a minimum.	Sec 1.4(c)	*25 years	(U) Details may also be protected by one or more

participants, off-net or on-net operations, CNE command, control and data exfiltration tools/capabilities and locations, used to exploit or maintain intrusive access to a target's IT/computer structure	See remarks for foreign releasability.			ECI. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
40. (S//SI//REL) Combination of details of individual aspects of CNE activities, that would allow a specific target to take specific counter-measures, such as: - Specific target network or device **and** - Specific capability, tool or technique used for exploitation of vulnerability	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4 (c)	*25 years	(U) Details may also be protected by one or more ECI. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.
41. (TS//SI//REL) The fact that NSA/CSS (or TAO) acquires cryptographic enabling information through CNE activities.	TOP SECRET//SI See remarks for foreign releasability.	Sec 1.4(c)	*25 years	(U//FOUO) Details may also be protected by one or more ECI and/or HCS. (U) Foreign releasability decisions handled on a case-by-case basis. Contact TAO CAO for further guidance.

(U) *25 years: Declassification in 25 years indicates that the information is classified for 25 years from the date a document is created or 25 years from the date of this original classification decision, whichever is later.

ACRONYMS/DEFINITIONS:

(U) **Computer Network Exploitation** (CNE): intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) or networks. (Per DCID 7/3, Information Operations and Intelligence Community Related Activities, effective 01 July 1999, administratively changed 5 June 2003)

(U) **Computer Network Attack** (CNA): operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Per DCID 7/3, Information Operations and Intelligence Community Related Activities, effective 01 July 1999, administratively changed 5 June 2003)

(U) **Computer Network Defense** (CND): efforts to defend against the CNO of others, especially that directed against U.S. and allied computers and networks. (Per DCID 7/3, Information Operations and Intelligence Community Related Activities, effective 01 July 1999, administratively changed 5 June 2003)

(U) **Computer Network Operations** (CNO): CNE, CNA, and CND collectively. (Per DCID 7/3, Information Operations and Intelligence Community Related Activities, effective 01 July 1999, administratively changed 5 June 2003)

(U) **Information Operations** (IO): actions taken to affect adversary information and information systems while defending one's own information and information systems. IO is an integrating strategy. (Per DCID 7/3, Information Operations and Intelligence Community Related Activities, effective 01 July 1999, administratively changed 5 June 2003)

(S//SI//REL) **Intrusive Access**: Refers to CNE operations involving remote manipulation, hardware/software modifications, or sensing of environment changes in a computer device or system, and/or occasionally the facilities that house the systems.

(S//SI//REL) **Off-Net Operations**: Refers to covert or clandestine field activities of personnel carried out in support of CNE activities.

(S//SI//REL) **Physical subversion**: Subverts with physical access to a device or host facility. Other terms sometimes used to connote physical subversion are close access enabling, exploitation, or operations; off-net enabling, exploitation, or operations; supply-chain enabling, exploitation, or operations; or hardware implant enabling, exploitation, or operations.

(S//SI//REL) **Remote subversion**: Subverts without physical access to a device or host facility; obtains unauthorized permission. Other terms sometimes used to connote remote subversion are computer network exploitation; endpoint access, exploitation, or operations; on-net access, exploitation, or operations; software implant access, exploitation, or operations; or accessing or exploiting data at rest.

(S//SI//REL) **Supply Chain Operations**: Interdiction activities that focus on modifying equipment in a target's supply chain.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu