NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

(U) CLASSIFICATION GUIDE FOR NSA/CSS QUANTUM COMPUTING RESEARCH 10-25

Effective Date: 21 September 2011

Revised Date(s):

CLASSIFIED BY: //s//
[redacted]

REASON FOR CLASSIFICATION: 1.4 (c), (g)
DECLASSIFY ON: 25 years*

ENDORSED BY: [redacted]

(U) Change Register

Change No.	Change	Date Made mm/dd/yy	By (initials)

CLASSIFICATION GUIDE TITLE/NUMBER: (U) NSA/CSS Quantum Computing Research, 10-25

PUBLICATION DATE: (U) 21 September 2011

OFFICE OF ORIGIN: (U) The Laboratory for Physical Sciences/R3

POC: (U//FOUO) [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: (U) [redacted], [redacted] [redacted]**, Community Integration, Policy and Records**

(U//FOUO) This document establishes information security guidelines on NSA/CSS-sponsored research in the field of quantum computing (QC). The objectives defining the scope of this research activity are:

> 1) (S//REL) To assess if it is to NSA's benefit to continue research into whether practical-scale QC can be developed within a reasonable timeframe, to identify its most promising physical embodiment(s), and to formulate a credible scenario for its large-scale development;
>
> 2) (U//FOUO) To gain an understanding of the computational cryptanalytic capabilities of quantum computers; and
>
> 3) (U//FOUO) To identify practical cryptographic methods that are not susceptible to quantum computational attack.

(S//REL) These guidelines *do not* cover the possibility of large-scale cryptologic QC development programs at NSA, but only the research and planning preliminary to, and in possible support of, such programs.

(S//SI//REL) Much of the research in quantum computing is still very basic and is most effectively pursued in NSA-funded open research programs. These programs play a critical role as the major source of new ideas and for training future researchers in the field. However, NSA is pursuing more than just basic, unclassified research. NSA is also attempting to preserve the SIGINT potential of quantum computing (i.e., the cryptanalytic applications of QC) while simultaneously attempting to protect the information security of both the Government and private sectors against hostile QC attacks (i.e., the cryptographic, mission assurance applications of QC of interest to the Information Assurance community). These goals must be pursued at the classified level.

(U//FOUO) There are several fundamental reasons for classifying QC research:

> 1) (TS//SI//REL) To protect NSA's efforts to develop cryptanalytic QC to attack high-grade public key encryption systems by denying adversaries information concerning NSA's assessment of, and/or plans for, large-scale QC development;

2) (S//REL) To enable us to track our adversaries' degree of success or failure in similar QC development efforts; and

3) (U//FOUO) To protect our own systems against adversarial cryptanalytic QC efforts.

(S//REL) Based on this, the distinctions between unclassified and classified information contained in this guide attempt to differentiate between unclassified basic-level, academic-scale research of scientific interest, and more comprehensive classified research which might disclose techniques that may otherwise be possible to protect, or which might imply, rightly or wrongly, serious intent on NSA's part to pursue large-scale development of cryptanalytic quantum computers.

Description of Information	Classification/ Markings	Category	Declass	Remarks
A. (U) General				
A.1. (U) The fact that NSA: • (U) Acknowledges the potential of Quantum Computing (QC) in the field of cryptanalysis. • (U) Tracks the development of QC technology. • (U) Conducts QC research. • (U) Funds selected QC research of unspecified external entities. • (U) Conducts and sponsors research in QC mathematics and algorithms, complexity theory, experimental physics, theoretical physics, control, and/or error correction. • (U) Discusses QC theory with unspecified external researchers within and outside the United States.	UNCLASSIFIED	N/A	N/A	(U) Details may require handling as UNCLASSIFIED//FOR OFFICIAL USE ONLY or may be classified.
A.2. (U//FOUO) The fact that NSA conducts *unspecified* classified research in QC with no additional details.	UNCLASSIFIED//FOR OFFICIAL USE ONLY	N/A	N/A	(U) Details may require classification and may be compartmented.
(U) Cooperation With Other Organizations				
A.3. (U//FOUO) The fact that NSA cooperates with other U.S. organizations (e.g., academic organizations, national laboratories, and other U.S. intelligence agencies) on basic, unclassified QC research without	UNCLASSIFIED	N/A	N/A	(U) Details, including specifying which U.S. organization, may require handling as UNCLASSIFIED//FOR OFFICIAL USE ONLY or may be classified.

additional details.				
A.4. (U//FOUO) The fact that NSA cooperates with the Second Party partners on basic, unclassified QC research without additional details.	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U//FOUO) Details, such as the particulars of research jointly undertaken by NSA and a specified Second Party partner, may be classified.
A.5. (U//FOUO) The fact that NSA cooperates with other U.S. organizations (e.g., academic organizations, national laboratories, and other U.S. intelligence agencies) or Second Party partners, on classified QC research.	UNCLASSIFIED// FOR OFFICIAL USE ONLY See Remarks	N/A	N/A	(U) Details, including specifying which U.S. organizations or Second Party partners, may be classified. Coordination with the other party may be required to arrive at a mutually-agreeable classification.
(U) Research Information				
A.6. (U) Details regarding or results of NSA-conducted or -sponsored unclassified research.	UNCLASSIFIED See Remarks	N/A	N/A	(U) Information is generally UNCLASSIFIED, except for information on breakthroughs. See A.12 below.
A.7. (U//FOUO) Non-technical details (e.g., scheduling) regarding NSA-conducted or -sponsored classified QC research.	CONFIDENTIAL// REL TO USA, FVEY at a minimum	1.4 (c)	25 years*	(U) Details may require higher classification.
A.8. (U//FOUO) Technical details regarding or results of NSA-conducted or -sponsored classified QC research.	SECRET//REL TO USA, FVEY at a minimum	1.4 (c)	25 years*	(U) Details (e.g., cryptanalytic applications) on specific research may require higher classification and/or compartmentation.
A.9. (U) The existence of a specific classified QC research project.	SECRET// REL TO USA, FVEY at a minimum	1.4 (c)	25 years*	(U) Higher classification and/or compartmentation may be required to protect specific projects.
A.10. (U//FOUO) Any information relating to a determination that QC is or is not cryptologically useful to NSA.	SECRET//REL TO USA, FVEY at a minimum See Remarks	1.4 (c)	25 years*	(U//FOUO) For example, the fact that NSA decides to fund or not to fund a specific classified QC research project would be classified SECRET//REL TO USA, FVEY or higher.
A.11. (U) The reason for a significant change in size or direction of the NSA QC research program.	CONFIDENTIAL// REL TO USA, FVEY at a minimum	1.4 (c)	25 years*	(U) Details may require higher classification and/or compartmentation.
(U) Breakthroughs				
A.12. (U//FOUO) The fact of or specific details of changes in NSA's understanding of the likelihood, timescale, required resources, or method of implementation of cryptanalytic-scale QC because of a breakthrough achieved through open research.	UNCLASSIFIED//FOR OFFICIAL USE ONLY at a minimum See Remarks	N/A	N/A	(U) Analysis by NSA of the significance of a breakthrough will normally require classification (generally at the S//SI//REL TO USA, FVEY level at a minimum) and/or compartmentation.
A.13. (U//FOUO) The fact of a change in NSA's understanding of the likelihood, timescale, required resources, or method of implementation of cryptanalytic-	SECRET//SI//REL TO USA, FVEY at a minimum See Remarks	1.4 (c)	25 years*	(U) Details and significance of the breakthrough may require higher classification and/or additional compartmentation.

scale QC because of a breakthrough achieved through classified research.				
A.14. (U//FOUO) The specific details of a change in NSA's understanding of the likelihood, timescale, required resources, or method of implementation of cryptanalytic-scale QC because of a breakthrough achieved through classified research.	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks	1.4 (c)	25 years*	(U) Details and significance of the breakthrough may require additional compartmentation (e.g., a method of implementation may leverage additional equities protected under a compartment).
B. (U) Level A/Level B QC Research				
B.1. (U) The fact that NSA conducts Level A and Level B QC research with no additional details. .	UNCLASSIFIED	N/A	N/A	(U) See the descriptions of Level A and Level B in the Definitions section.
B.2. (U//FOUO) The fact that Level A is unclassified QC research and/or Level B is classified QC research.	UNCLASSIFIED//FOR OFFICIAL USE ONLY	N/A	N/A	
B.3. (S//REL) The fact that NSA defines specific limits to distinguish Level A QC research from Level B QC research.	SECRET//REL TO USA, FVEY	1.4 (c)	25 years*	
B.4. (S//REL) The specific values distinguishing Level A QC research from Level B QC research.	SECRET//REL TO USA, FVEY	1.4 (c)	25 years*	(U//FOUO) The values are expected to change over time based on achievements in the open community.
C. (U) QC Algorithm Research				
C.1. (U) The fact that NSA-conducted or -sponsored unclassified research has achieved a quantum algorithm improvement of an unclassified classical algorithm with polynomial run-time.	UNCLASSIFIED at a minimum See Remarks	N/A	N/A	(U//FOUO) Publically known algorithms are generally unclassified. However, because of their relevance to NSA's QC effort or cryptanalytic capabilities, improvements to an unclassified algorithm may be protected as determined on a case-by-case basis. Contact guide POC. (U) General algorithm research falls under this category.
C.2. (U) The fact that NSA-conducted or -sponsored unclassified research has achieved a quantum algorithm improvement of an unclassified classical algorithm yielding a polynomial speed-up.	UNCLASSIFIED at a minimum See Remarks	N/A	N/A	(U//FOUO) Publically known algorithms are generally unclassified. However, because of their relevance to NSA's QC effort or cryptanalytic capabilities, improvements to an unclassified algorithm may be protected as determined on a case-by-case basis. Contact guide POC. (U//FOUO) A polynomial speed-up of an unclassified algorithm may make some intractable cryptanalytic problems tractable.

C.3. (U) The fact that NSA-conducted or -sponsored unclassified research has achieved a quantum algorithm improvement of a classical algorithm yielding a super-polynomial speed-up.	UNCLASSIFIED at a minimum See Remarks	N/A	N/A	(U//FOUO) Publically known algorithms are generally unclassified. However, because of their relevance to NSA's QC effort or cryptanalytic capabilities, improvements to an unclassified algorithm may be protected as determined on a case-by-case basis by the originating Agency. Contact guide POC. (U) For example, a polynomial time algorithm for solving Graph Isomorphism.
C.4. (U//FOUO) The fact that NSA has determined that a specific classical public-key cryptography design is or is not secure against QC attack where the security or non-security of the algorithms *is* widely known and publicly available.	UNCLASSIFIED	N/A	N/A	(U) For example, it is known that QC breaks cryptosystems based on RSA, Diffie-Hellman, and elliptic curve cryptosystems. (U) For assistance in determination, contact guide POC.
C.5. (U//FOUO) The fact that NSA has determined that a specific classical public-key cryptography design is or is not secure against QC attack for algorithms for which the security or non-security *is not* widely known and publicly available.	SECRET//REL USA, FVEY at a minimum See Remarks	1.4 (c)	25 years*	(U) Specific designs may require higher classification and/or compartmentation
D. (U) Programs and Plans				
D.1. (TS//SI//REL) The existence or nonexistence of any NSA plan or program to build a cryptanalytic-scale quantum computer.	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks	1.4 (c)	25 years*	(U) Details indicating specific planning or program development may require compartmentation.
E. (U) Information Assurance				
E.1. (U) The fact of a vulnerability of a specific U.S. Government cryptosystem to QC attack.	TOP SECRET See Remarks	1.4 (c)(g)	25 years*	(U) Refer to the Information Assurance Vulnerabilities and Weaknesses Classification Guide, 3-02, 8 July 2005, concerning foreign releasability of information on cryptanalytic vulnerabilities of U.S. systems.
E.2. (U) The fact that NSA is attempting to design classical public-key cryptography that is secure against QC attack.	UNCLASSIFIED See Remarks	N/A	N/A	(U) Details may require handling as UNCLASSIFIED//FOR OFFICIAL USE ONLY or may be classified.
F. (U) Materials				
F.1. (U) The fact of NSA involvement in developing specialized materials for unclassified QC that would not	UNCLASSIFIED	N/A	N/A	

involve developing specialized production facilities.				
F.2. (S//SI//REL) The fact of NSA involvement in developing specialized materials for classified cryptanalytic QC.	SECRET//SI//REL TO USA, FVEY See Remarks	1.4 (c)	25 years*	(S//SI//REL) Such development might include, but is not limited to, isotopic or impurity purification, defect reduction, and/or surface passivation.
F.3. (S//SI//REL) The fact of NSA involvement in developing specialized materials for classified cryptanalytic QC that would involve developing or using specialized production facilities or prototypes of such facilities.	SECRET//SI//REL TO USA, FVEY See Remarks	1.4 (c)	25 years*	(S//SI//REL) Development of such production plants indicates a level of NSA commitment to cryptanalytic QC development beyond unclassified research.
F.4. (S//SI//REL) Technical details regarding NSA development of specialized materials for cryptanalytic QC.	SECRET//SI// REL TO USA, FVEY at a minimum See Remarks	1.4 (c)	25years*	(S//SI//REL) Resulting specialized materials will generally be handled as SECRET//SI// REL TO USA, FVEY; exceptionally high-purity material or experimental results may require protection as TOP SECRET//SI//REL TO USA, FVEY.

* (U) 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.

(U) DEFINITIONS

(U) **Cryptanalysis -** The study of breaking codes and ciphers.

(S//SI//REL) **Cryptanalytic-Scale -** (as applied to quantum computers) Large enough to perform computations of actual cryptanalytic importance to NSA. A more specific definition is likely to be compartmented, and will change over time.

(U) **Cryptography -** The principles, means, and methods for rendering plain information unintelligible to the uninitiated and for restoring encrypted information to intelligible form.

(U) **Cryptology -** The art and science of making codes/ciphers and breaking them,. Cryptology breaks out into two disciplines: cryptography (making or using codes/ciphers) and cryptanalysis (breaking codes/ciphers).

(U) **Detailed engineering design -** Specifications of a set of qubits and the associated initialization, control, and measurement hardware and software at a level of detail commensurate with the requirements of industrial fabrication.

(U) **Fidelity -** Precision of qubit operations such as initialization, logic gates, and readout.

(U) **High-fidelity *N*-qubit Device -** An engineered processing device that integrates *N* coupled, high-fidelity physical qubits, i.e., qubits with fidelity of operations near or beyond the accuracy threshold for efficient error correction.

(S//REL) **Level A QC -** Unclassified theoretical and/or experimental research in the design, physical implementation, and operation of quantum computers, as established by the Laboratory for Physical Sciences/R3.

(S//REL) **Level B QC -** Classified theoretical and/or experimental research in the design, physical implementation, and operation of quantum computers, as established by the Laboratory for Physical Sciences/R3. The boundaries are based on the number and quality of qubits, realism and specificity of design, control precision, and detail of analysis. While these boundaries may change over time, as of the publication of this guide, the values are:

(1) (S//REL) Detailed engineering design of 51 or more physical qubits;

(2) (S//REL) Implementation and operation of a high-fidelity 21-or-more physical-qubit device; or

(3) (S//REL) Implementation and operation of three (3) or more logical qubits, with sufficient speed and precision to allow preservation of quantum information and logical gates between the qubits.

(U) **Logical qubits -** Collections of several physical qubits configured in a circuit allowing detection and correction both of errors and of loss of quantum coherence.

(U) For the purposes of this guide, the circuit configuration of a logical qubit must allow detection and correction of at least all errors affecting any single physical qubit. A logical qubit comprising *N* physical qubits must also be a high-fidelity *N*-qubit device.

(U) **Physical qubit -** A physical entity capable of storing a qubit of information and being initialized, operated on, and measured. Examples include, but are not limited to: photons, electrons, atoms, atomic nuclei, and superconducting Josephson junctions.

(S//SI//REL) **Practical-Scale -** Cryptanalytic-scale, with the added requirement that a roadmap exists to construct the device with a cost, probability of success, and time-scale of actual cryptanalytic importance to NSA. A more specific definition is likely to change over time.

(U) **Quantum coherence -** The fundamental quantum-mechanical property of qubits and collections of qubits which may enable some computations to be performed with resources vastly smaller than would be required for classical computers.

(U) **Quantum Computing -** Computing with quantum operations on data stored in a collection of qubits.

(U) **Quantum gates -** Logic operations on one or more qubits that preserve their quantum coherent character.

(U) **Qubit -** A “quantum bit,” the fundamental unit of information in a quantum computer.