Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (U//~~FOUO~~)

1. (U//~~FOUO~~) Purpose

(U//~~FOUO~~) This document establishes policy and responsibilities for disseminating information about vulnerabilities discovered by the United States Government (USG) or its contractors, or disclosed to the USG by the private sector or foreign allies in Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS), or other commercial information technology or industrial control products or systems (to include both hardware or software). This policy defines a process to ensure that dissemination decisions regarding the existence of a vulnerability are made quickly, in full consultation with all concerned USG organizations, and in the best interest of USG missions of cybersecurity, information assurance, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection.

2. (U//~~FOUO~~) Scope

(U//~~FOUO~~) This Policy applies to all components, civilian and military personnel, and contractors of the United States Government and to all hardware and software employed on government networks to include Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS), or other commercial information technology or industrial control products or systems (to include open-source software). Industrial Control Systems (ICS) and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) have a significant impact on the reliability and safe operation of the Critical Infrastructure / Key Resources (CI/KR)[1] and are also included.

(U//~~FOUO~~) It is not the intent of this policy to prevent any USG entity from taking immediate actions to protect its network(s) from active intrusions based on vulnerabilities or to restrict those organizations responsible for warning USG entities about cyber attacks or intrusions from warning those entities who are actively being penetrated. Other significant equities associated with adversary exploitation of vulnerabilities on USG networks are beyond the scope of the process set forth below.

(U//~~FOUO~~) Nothing in this policy supersedes existing U.S. laws, regulations, Executive Orders, and directives to protect National Security Systems, Sensitive Compartmented Information, or other U.S. Government systems and information.

3. (U//~~FOUO~~) Background

~~(S//REL USA, FVEY)~~ (U//~~FOUO~~) The *Joint Plan for the Coordination and Application of* [redacted] *to Defend U.S. Information Systems*, produced in accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, *Cybersecurity Policy*, sets forth the following task: (b) (1) (b) (3)

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3)

[1] As defined in Homeland Security Policy Directive 7.

[redacted] (b) (5)

[redacted] (b) (1) (b) (3)

(U//~~FOUO~~) While the aforementioned task speaks of commercial information technology, an analogous situation applies with regard to government-developed information technology products or systems. Therefore, as noted above, this policy applies to such products or systems as well.

4. (U//~~FOUO~~) Equities

~~(S//REL USA, FVEY)~~ (U//~~FOUO~~) As stated in the task, the discovery of vulnerabilities [redacted] (b) (1) (b) (3) Therefore, actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these 'equities' are addressed." Several USG departments and agencies have recognized the vulnerability equities challenge and developed individual policies and processes for their resolution, sometimes involving other agencies known to have similar interests. However, to date there has been no comprehensive common policy and systematic process for handling the problem across the USG. This policy has been developed drawing upon the experiences of existing agency processes and addresses these challenges. A discussion of community equities can be found in Annex A.

5. (U//~~FOUO~~) Policy

~~(S//REL USA, FVEY)~~ USG entities shall appropriately classify and/or designate for special handling, in accordance with their own department/agency classification guidance and policy, vulnerabilities discovered by the USG or by non-USG entities under contracts with the USG, or disclosed to the USG by the private sector or foreign allies prior to entry into this process. In some circumstances, information may be unclassified yet designated as Protected Critical Infrastructure Information (PCII) and will be afforded protection under the DHS PCII rules and programs. The designation or classification may be formally changed during the process. Classification decisions may necessarily identify information as Protected Critical Infrastructure Information (PCII) requiring special handling. The fact that a vulnerability exists, and the risk information relating to a vulnerability, will be classified in accordance with applicable national security classification guidelines.

(U//~~FOUO~~) USG entities shall introduce any such vulnerability discovered into the following Vulnerabilities Equities Process (VEP).

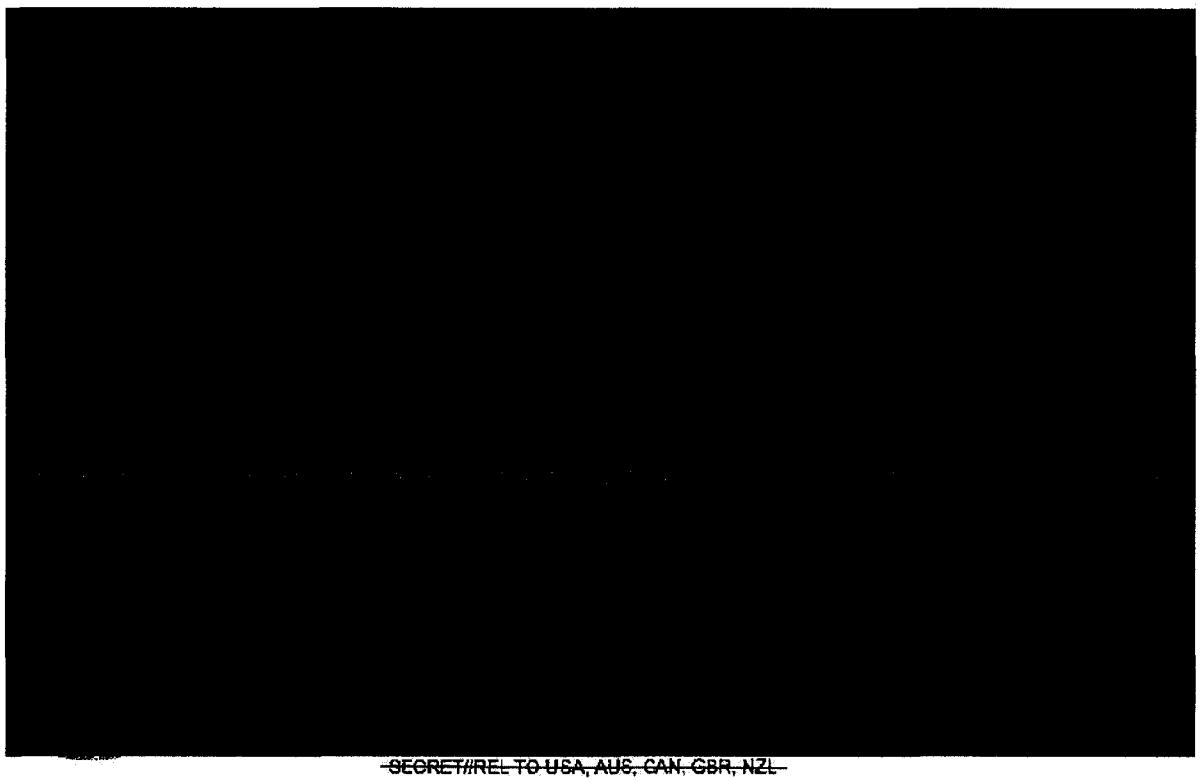
~~(S//REL USA, FVEY)~~ USG entities will restrict the dissemination external to the USG of any such vulnerability until such time as the following VEP is applied.

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3)

~~(S//REL TO USA, FVEY)~~ [redacted] (b) (1) (b) (3)

6. (U//~~FOUO~~) Vulnerability Equities Process

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~



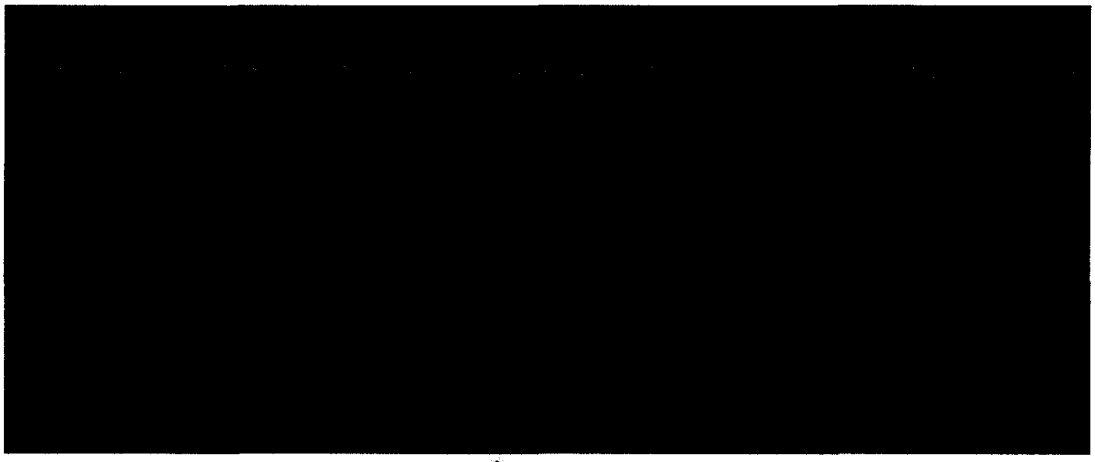
(b) (1)
(b) (3)

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

6.1. (U//~~FOUO~~) Process Overview

~~(S//REL USA, FVEY)~~ Figure 6.1 outlines the Vulnerability Equities Process. Expanded details for each step in the process are described in Sections 6.2-6.7 below. To summarize, when a vulnerability is identified from whatever source, the following process will be initiated:

a.
b.
c.
d.



(b) (1)
(b) (3)

[redacted] (b) (5)

e. [redacted] (b) (1) (b) (3)

f. [redacted]

6.2. (U//~~FOUO~~) Process Considerations

(U//~~FOUO~~) The VEP must be used before any vulnerability information is provided to entities other than those participating in the process. However:

a. (U//~~FOUO~~) Vulnerabilities discovered before the effective date of this process need not be put through the process. USG entities may voluntarily submit vulnerabilities discovered prior to the effective date that meet threshold requirements, and are expected to do so for vulnerabilities that they judge may present especially significant security risks.

b. ~~(S//REL TO USA, FVEY)~~ [redacted] (b) (1) (b) (3)

c. (U//~~FOUO~~) [redacted] (b) (3)

d. (U//~~FOUO~~) Vulnerabilities identified during the course of federally-sponsored open and unclassified research, whether in the public domain or at a government agency, FFRDC, National Lab, or other company doing work on behalf of the USG need not be put through the process. Information related to such vulnerabilities, however, does require notification to the Executive Secretariat, which shall notify process participants for purposes of general USG awareness.

e. (U//~~FOUO~~) Vulnerabilities discovered during an evaluation requested by a USG entity may be disclosed to that specific entity concurrently with entry into the VEP.

f. (U//~~FOUO~~) If a vulnerability is found in a GOTS equipment or system that was certified by NSA, or in any cryptographic function, whether in hardware or software, certified or approved by NSA, then the vulnerability will be reported to NSA as soon as practicable. NSA will assume responsibility for this vulnerability and submit it formally through the VEP as appropriate.

[redacted] (b) (5)

g. ~~(S//REL TO USA, FVEY)~~ [redacted] (b) (1) (b) (3)

6.3. ~~(U//FOUO)~~ Process Participants

~~(S//REL USA, FVEY)~~ Each USG entity participating in the VEP will designate a department/agency VEP POC. The VEP POCs will be responsible for submitting vulnerabilities into the process and will be the primary contact with the VEP Executive Secretariat. Organizational VEP POCs are responsible for ensuring that applicable cybersecurity, cyber defense, information assurance, intelligence, counterintelligence, law enforcement, [redacted] of their organization are appropriately represented in the process. (b) (1) (b) (3)

(U) [redacted] (b) (5)

~~(S//NF)~~ [redacted] (b) (1) (b) (3)

(U) Other participants may include the Departments of State, Justice, Homeland Security, Treasury, Commerce, and Energy, and the Office of the Director of National Intelligence when they have self-identified equities with regard to the vulnerability under discussion.

6.4. (U//~~FOUO~~) Threshold for Entering VEP

(U//~~FOUO~~) The USG entity will apply the following 'threshold' to identify whether or not the vulnerability should enter the process: to enter the process a vulnerability must be both newly discovered and not publicly known. (As stated above, vulnerabilities discovered before the effective date of this process need not be put through the process. However, Departments/Agencies may voluntarily submit vulnerabilities discovered prior to the effective date.)

6.5. (U//~~FOUO~~) Executive Secretariat

(U//~~FOUO~~) The National Security Agency/Information Assurance Directorate will serve as the Executive Secretariat for the process. Such function will be executed so as to remain neutral and independent of the organization's equities in any particular case. The Executive Secretariat shall facilitate information flow, SME discussions, ERB decisions, and documentation and recordkeeping for the process. The Executive Secretariat shall keep formal records of this information to permit later review of the overall efficacy of the process. A discussion of the roles and responsibilities of the Executive Secretariat can be found in Annex B. The Secretariat role may be assigned to another core department or agency after annual review per section 7 below.

[redacted] (b) (5)

6.6. (U//~~FOUO~~) Notification and Vulnerability Equities Discussion

6.6.1. (U) Notification and Discussion Timeline.

a. (U) The Executive Secretariat will distribute the vulnerability information to participants no later than the close of business on the work day following its receipt of notification from the originating participant.

b. ~~(S//REL USA, FVEY)~~ The vulnerabilities equities discussion will begin [redacted] of notification to the participants. [redacted] the ERB will reach a decision or, if it is unable to reach a decision, will refer the matter to [redacted]. In the event a USG entity holding an equity in the issue disagrees with the decision of the ERB, it may appeal the ERB's decision to [redacted] A request for such an appeal will be submitted to the Executive Secretariat [redacted] following the ERB's decision as set forth in section 6.7.1. (b) (1) (b) (3) (b) (5) (b) (5) (b) (5)

c. ~~(S//REL USA, FVEY)~~ If a USG entity discovers a new vulnerability that is associated with an active cyber attack or cyber exploitation against a USG system or U.S. Critical Infrastructure/Key Resource (CI/KR) system, the entity will report it immediately to the Executive Secretariat. [redacted] This policy is not intended to prevent any organization from taking immediate actions to protect its network(s). Every attempt will be made by the defense community to identify an immediate mitigation strategy and to convey this to the affected USG entity. (b) (1) (b) (3)

d. (U) Participants may also request expedited handling of other special cases.

6.6.2. (U) Discussion Procedures

(U//~~FOUO~~) Vulnerability information may be released to cleared individuals from organizations within the VEP for purposes of carrying out the process.

(U) The SMEs will formulate a recommendation for submission to the ERB. Consultation with outside experts is permitted on an as-needed basis. Outside experts must have requisite security clearances and/or adhere to the non-disclosure agreements of each organization with an equity in the case under consideration.

~~(S//REL USA, FVEY)~~ The classification of the vulnerability may be readdressed during this phase of the VEP. The SME discussion may include a review of classification guidance associated with data related to a specific vulnerability and may result in a recommendation to the ERB for potential reclassification guidance. Any ERB endorsed reclassification guidance decision would be forwarded by the Executive Secretariat to relevant USG Original Classification Authority(s).

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3)

6.7. (U) Decision-Making

~~(S//NF)~~ An interagency Equities Review Board (ERB) will be established, under the auspices of the [redacted] (b) (5)
[redacted] (b) (1)
(b) (3)

a. (U//~~FOUO~~) For any specific equity case, additional departments and agencies may identify their equities and be invited to participate for that case, subject to classification constraints and the provisions of this policy. Any representative participating on the ERB shall have the authority to make decisions on his/her agency's behalf.

b. ~~(S//REL USA, FVEY)~~ Attendance at ERB meetings will be tightly controlled to allow discussion of equities in a trusted environment. All representatives will be required to possess appropriate clearances.

c. (U//~~FOUO~~) Ideally, the ERB will ratify recommendations made by the SME discussions. If consensus cannot be reached by the ERB, decision will be by majority vote.

d. (U//~~FOUO~~) At its discretion, the ERB may opt to establish a streamlined business process by which a unanimous recommendation of the SMEs to disseminate a vulnerability need not be raised to the ERB but would take effect immediately upon recording of that unanimous recommendation by the Secretariat.

6.7.1. (U//~~FOUO~~) Appeals (b) (5)

~~(S//REL USA, FVEY)~~ It is the intent of the VEP for decisions to be made by the ERB whenever possible. Nevertheless, ERB decisions may be appealed to [redacted]. An ERB member wishing to appeal a decision shall notify the Executive Secretariat, which will notify [redacted]. The Executive Secretariat will notify [redacted] of each ERB decision; if a policy concern arises [redacted] will arrange for further discussion with the ERB. The [redacted] will arrange for the [redacted] to consider appeals when necessary.

6.8. (U//~~FOUO~~) Decision Implementation

~~(S//REL USA, FVEY)~~ In most cases, implementation responsibilities will vary according to the specific decision made by the ERB or [redacted] Throughout, responsible parties will document to the Executive Secretariat the steps taken and any known results or further developments. In addition, the responsible party will provide the Executive Secretariat and other participants in the process (including overseers) further information on implementation upon request. (b) (5)

6.8.1. (U//~~FOUO~~) Decision Implementation: Restrict Dissemination

~~(S//REL USA, FVEY)~~ [redacted] (b) (1)
(b) (3)

[redacted] (b) (5)

[redacted] (b) (1) (b) (3)

6.8.2. (U//~~FOUO~~) Decision Implementation: Disseminate

(~~S//REL USA, FVEY~~) When a decision is made to disseminate information pertaining to the vulnerability, the ERB will establish guidelines for disseminating that information, including mitigation strategies, to the cyber security centers that are primarily responsible for defending or coordinating the defense of networks and systems [redacted] (b) (1) (b) (3)

(~~S//REL USA, FVEY~~) In the event that a vulnerability was discovered through intelligence activities or the information about a vulnerability contains US Person or Sources and Methods Information, dissemination must be accomplished in accordance with all existing laws, regulations, Executive Orders, directives, and rules governing the dissemination of such information. Efforts will be made to downgrade the classification level of the vulnerability so that dissemination is possible.

(U) In accordance with HSPD-7, DHS will coordinate the distribution of allowed vulnerability information to its partners and customers which may include Federal departments/agencies (e.g. Sector Specific Agencies and members of Government Coordinating Councils for the relevant CI/KR sectors); State, local and tribal governments, the private sector, academia and international partners. Information dissemination shall be in accordance with the ERB decision.

(U) In accordance with existing DoD policy, the DoD will lead the dissemination of such information pertaining to vulnerabilities to DoD networks. Information dissemination shall be in accordance with the ERB decision.

(U) In accordance with National Security Directive-42 and E.O. 13231, the Committee on National Security Systems (CNSS), and NSA, in its role as the National Manager for national security systems, will lead the dissemination of such information to the national security community.

(U) In accordance with existing Intelligence Community – Incident Response Center (IC-IRC) vulnerability management procedures derived from the Director of National Intelligence and the Intelligence Community Chief Information Officer's statutory authorities contained in the National Security Act of 1947 as amended, the IC-IRC will lead the dissemination of such information pertaining to vulnerabilities to IC networks. Information dissemination shall be in accordance with the ERB decision.

7. Oversight

(~~S//REL USA, FVEY~~) Annual reporting on implementation will be done by the Executive Secretariat and submitted to the participants [redacted] (b) (5)

(U//~~FOUO~~) Departments and agencies will report to the Executive Secretariat the following in order to facilitate the production of the annual report:

a. Parties or communities (vendors, customers, databases) that received the information,

b. When the information was disseminated,

c. Any significant known further developments, including whether the vulnerability is currently being exploited on USG or critical infrastructure/key resource systems.

d. An assessment on the degree of usefulness to the recipient communities that received the information,

e. Mitigations and dissemination of mitigation information,

f. Use of this vulnerability information in sensor development, and

g. Other data which the Executive Secretariat may request in support of the reports detailed in the following section.

~~(S//REL USA, FVEY)~~ Reports should support assessment of the process for:

a. Relevance: utility for the most common scenarios,

b. Effectiveness of the threshold for what comes into the process,

c. Trust: how well it is trusted by participating organizations,

d. Encouraging pursuit of mutually beneficial solutions,

e. Timeliness of decisions,

f. Frequency of appeals,

g. Whether work & resources required are proportionate to the benefits,

h. Effectiveness of recordkeeping,

i. Consistency of decision-making,

j. Criticality of decision,

k. Appropriateness of representatives in the process,

l. Effectiveness of mitigations and corrective measures,

m. Effectiveness of dissemination processes regarding the vulnerabilities themselves, mitigations and fixes, as appropriate,

n. [redacted]

o.

(b) (1)
(b) (3)

~~(S//REL USA, FVEY)~~ Reports may recommend changes/adjustments to the process. This process will be reviewed annually.

[redacted] (b) (5)

(U) Annex A - Equities

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3)

(U//~~FOUO~~) Defensive Cyber Operations Community Equities. The defensive cyber operations community and information assurance community, executing their defense mission areas, may desire to notify USG, industry, and critical infrastructure partners as well as allies of the vulnerability as it develops appropriate patches and mitigation strategies to address a vulnerability.

(S//REL USA, FVEY)

~~(S//FOUO~~ [redacted] (b) (1) (b) (3)

~~(S//REL USA, FVEY~~ [redacted] (b) (1) (b) (3)

~~(S//REL USA, FVEY)~~ Other Equities. Some USG entities may not have equities that fall under those mentioned but, while executing their roles/responsibilities, they will be affected by the vulnerability or they have responsibilities that should be considered as part of the decision process (e.g. Department of State, Department of Energy, Department of Commerce, *et al*).

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3)

(U) Annex B – Roles and Responsibilities

(U) Vulnerability Equities Process (VEP) Points of Contact (POC) – Designated by each participating USG entity, the POC may be a section or person within that USG entity and will act as the focal point for vulnerability discovery and notification into the VEP.

(U) VEP Subject Matter Experts (SME) – Designated by each participating USG entity, the SMEs will act as the department or agency representatives in the equities discussion. Depending on the department or agency, one or more SME may be identified.

(U) Equities Review Board (ERB) Members – Designated by each participating USG entity, ERB members will be senior level department/agency representatives empowered by that department/agency to vote on its behalf. Each department/agency will have only one ERB member with two designated alternates.

(U) Executive Secretariat – Specific duties of the Executive Secretariat include:

- Maintain VEP POC, SME, and ERB member contact information.
- Maintain records of all vulnerabilities that have been identified to the Executive Secretary and all vulnerabilities considered by the process Recorded information will include at a minimum when discovered, by whom, VEP decision reached, when the vulnerability is up for review, and other information received from the participants.
- Document and maintain files on the appellate process.
- Create an annual report. The report will be submitted to the participants [redacted] (b) (5)

(U) Annex C - Definitions

(U) Commercial, off-the-shelf (COTS) – A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.

(U) External Dissemination – The sharing or release of vulnerability information to entities external to the USG.

(U) Government off-the-shelf (GOTS) – A software and/or hardware product that is developed by the technical staff of a government agency for use by the USG. GOTS software and hardware may be developed by an external entity, but with funding and specification from the agency, and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the government.

(U) Industrial Control System (ICS) – A term that encompasses several types of control systems to include Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. ICSs are typically used in industries such as electricity, water, oil, and gas distribution. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

(U) National security systems –As set forth in 44 U.S.C. 3542(b)(2):

> (2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
>
> (i) the function, operation, or use of which—
>
> (I) involves intelligence activities;
>
> (II) involves cryptologic activities related to national security;
>
> (III) involves command and control of military forces;
>
> (IV) involves equipment that is an integral part of a weapon or weapons system; or
>
> (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
>
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
>
> (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(U) Publicly known – A vulnerability is deemed to be publicly known if the source of the information is a verbal or electronic presentation or discussion in a publicly accessible domain, or if there is a paper or other published documentation in the public domain (e.g., that which could be easily found on the Internet, in trade journals, etc.) that specifically discusses the vulnerability under consideration and how the vulnerability could be exploited. This definition does NOT include information currently and properly protected as U//FOUO or classified that has been inappropriately released to the public.

[redacted] (b) (5)

(U//FOUO) Vulnerability – A technical design or implementation flaw in an Industrial Control System, Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS), or other commercial information technology product or systems that could potentially be used to exploit or penetrate a product or system (hardware or software, to include open-source software).