Vulnerabilities Equities Policy and Process for the United States Government

November 15, 2017

1. Purpose

This document describes the Vulnerabilities Equities Policy and Process for departments and agencies of the United States Government (USG) to balance equities and make determinations regarding disclosure or restriction when the USG obtains knowledge of newly discovered and not publicly known vulnerabilities in information systems and technologies. The primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes.

The Vulnerabilities Equities Process (VEP) balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence. The U.S. Government's determination as to whether to disseminate or restrict a vulnerability is only one element of the vulnerability equities evaluation process and is not always a binary determination. Other options that can be considered include disseminating mitigation information to certain entities without disclosing the particular vulnerability, limiting use of the vulnerability by the USG in some way, informing U.S. and allied government entities of the vulnerability at a classified level, and using indirect means to inform the vendor of the vulnerability. All of these determinations must be informed by the understanding of risks of dissemination, the potential benefits of government use of the vulnerabilities, and the risks and benefits of all options in between. This document defines the policy and process for evaluating competing considerations to inform U.S. Government decisions.

2. Background

In accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, Cybersecurity Policy, and the *Joint Plan for the Coordination and Application of Offensive Capabilities to Defend U.S. Information Systems*, the USG created the VEP.

In the course of carrying out USG missions, the USG may identify vulnerabilities that cyber actors could exploit. In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. However, there are legitimate advantages and disadvantages to disclosing vulnerabilities, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time or adopting a mitigation strategy short of full disclosure can have significant consequences.

It is also important to recognize that the USG has not created these vulnerabilities. Information systems will continue to have vulnerabilities and efforts to discover and disclose these flaws is an ongoing need. Contributions by the Intelligence Community (IC) have been significant in securing modern information technology. If the USG were to adopt a policy of immediate disclosure, there would still be vulnerabilities present that would be discovered and potentially exploited by other cyber actors. For years, the USG's process to robustly consider and disclose vulnerabilities was the only such process known amongst both our peers and our adversaries.

Vulnerabilities can have significant economic, privacy and national security implications when exploited. The USG and the private sector are at risk due to our dependency on cyberspace. The USG is committed to an open, interoperable, secure, and reliable Internet and understands vulnerabilities in technologies underpinning the Internet threaten both security and liberty. Any system, including those we rely on for critical infrastructure, can be a target for malicious cyber activity. Interests in protecting the public from criminal cyber intrusions are often implicated by decisions to restrict or disseminate a vulnerability, particularly in the absence of meaningful mitigation. Unpatched vulnerabilities leave not only USG systems, but also the systems of commercial industry and private citizens, vulnerable to intrusion.

Vulnerabilities are also used in the course of authorized military, intelligence, and law enforcement activities. At times, intelligence and evidence discovered through judicious exploitation of a vulnerability are the only means to understand a much bigger threat. Often taking a considered risk to restrict knowledge of a vulnerability is the only way to discover significant intrusions that are compromising security and privacy.

For these reasons, vulnerability disclosure raises a multitude of considerations that require careful deliberation through an interagency process with a diversity of viewpoints. Competing USG missions require coordination and collaboration to protect information systems and citizens from malicious cyber activity. Additionally, the USG must be able to conduct law enforcement, military and intelligence activities to the fullest extent practical and in accordance with the laws that govern these activities.

Since there can be competing considerations for disclosing or restricting a vulnerability, it is important that the equity process be led outside any single agency. For this reason, the process is coordinated by the National Security Council (NSC) staff so that multiple agency viewpoints can be considered, informed by the full input and consideration of the interagency experts.

3. Scope

This policy supersedes the *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, dated February 16, 2010. Otherwise, nothing in this policy is meant to supersede existing U.S. laws, regulations, executive orders, and directives to protect National Security Systems (NSS), Sensitive Compartmented Information, or other

USG systems and information. This policy will be implemented consistent with the statutory authorities and responsibilities of the heads of participating agencies.

This policy applies to all USG components and personnel (i.e., civilian, military, and contractors) and includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

This policy is not intended to prevent the USG from taking immediate actions to protect its network(s) or warn entities actively threatened by a malicious cyber event, including ongoing unauthorized access to information systems.

4. Participation in VEP

4.1. Equities Review Board and VEP Director

The Equities Review Board (ERB) is the primary forum for interagency deliberation and determinations concerning the VEP. The ERB will meet monthly, but may also be convened sooner if an immediate need arises.

The ERB will consist of representatives from the following agencies who are authorized to represent the views of their respective agency head:

- Office of Management and Budget
- Office of the Director of National Intelligence (to include Intelligence Community-Security Coordination Center (IC-SCC))
- Department of the Treasury
- Department of State
- Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force (NCIJTF))
- Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS))
- Department of Energy
- Department of Defense (including the National Security Agency (NSA) (including Information Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber Crime Center (DC3))
- Department of Commerce
- Central Intelligence Agency

Other USG agencies may participate when demonstrating responsibility for, or identifying equity in, a vulnerability under deliberation. Changes to the name of an agency will not affect its participation in this process.

Each agency participating in the VEP will designate an agency point of contact (POC) to act as the focal point for vulnerability submissions for their respective organization and the primary contact for the VEP Executive Secretariat.

The VEP POC will ensure one or more Subject Matter Experts (SME) from their agency are identified to support equities determinations and discussions as needed.

The VEP Director at the NSC will be responsible for ensuring effective implementation of VEP policies. The VEP Director is the Special Assistant to the President and Cybersecurity Coordinator, or an equivalent successor.

4.2. VEP Executive Secretariat

The NSA will support VEP governance by serving as the Executive Secretariat for the VEP, acting at all times under the authority, direction, and control of the Secretary of Defense. The VEP Director may designate another agency to perform this function with the permission of the head of that agency. The VEP Executive Secretariat function will be executed so as to remain neutral and independent.

The VEP Executive Secretariat will facilitate information flow, discussions, determinations, documentation, and recordkeeping for the process. The VEP Executive Secretariat will keep formal records of this information to permit later review of the overall efficacy of the process.

Specific duties of the VEP Executive Secretariat include:

- Maintain VEP POC, SME, and ERB member contact information.
- Maintain records of all vulnerabilities that have been identified to the VEP Executive Secretariat. At a minimum, records will include the submitting agency, the dissemination determination and date, and whether reassessment is necessary. Other pertinent information may also be recorded.
- Create an annual report as described in Section 4.3.
- Document and maintain records of the contested preliminary determination process described in Section 5.2.6.

4.3. Annual Reporting

The VEP Executive Secretariat will produce an annual report that will be submitted to the VEP POCs and the NSC staff through the Special Assistant to the President and Cybersecurity Coordinator, or an equivalent successor. The report will be written at the lowest classification level permissible and will

include, at a minimum, an executive summary written at an unclassified level. As part of a commitment to transparency, annual reporting may be provided to the Congress.

The annual report will include statistical data as deemed appropriate by the VEP Director for the reporting period beginning on October 1 and ending on September 30. Changes, if any, to the following will also be included in the annual report:

- ERB membership.
- Reassignment of the VEP Director responsibility to another position.
- Realignment of the VEP Executive Secretariat responsibility to another agency.

5. Process

5.1. Threshold for Entering VEP

Agencies will submit vulnerabilities that meet the threshold. To enter the process, a *vulnerability* must be both *newly discovered* and *not publicly known* in accordance with the definitions in Annex A.

5.2. Workflow

Figure 1 outlines the Vulnerability Equities Process that will be initiated when a vulnerability is identified for equities review.

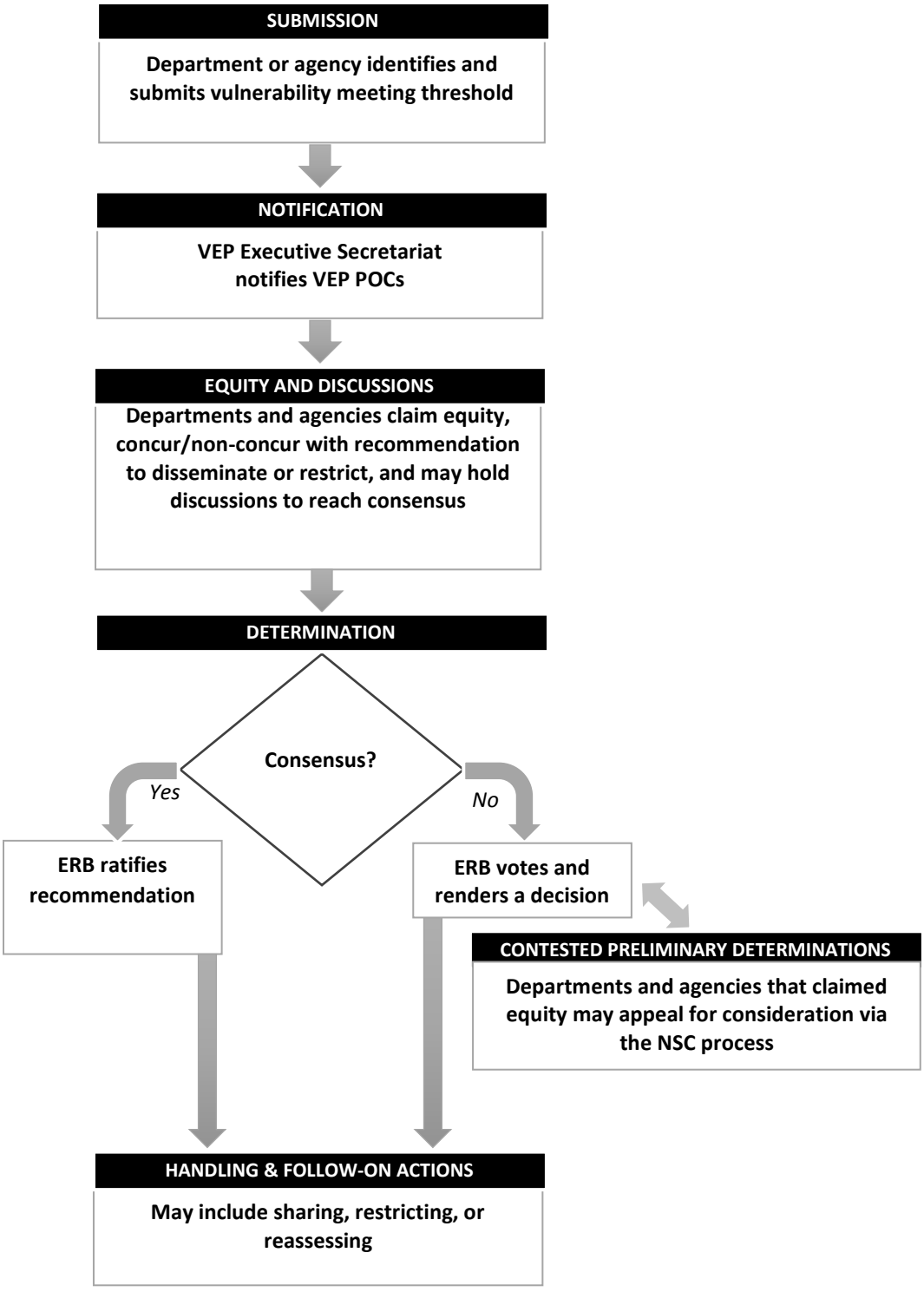

Figure 1: Vulnerability Equities Process Overview

5.2.1. Submission

When an agency determines that a vulnerability reaches the threshold for entry into the process, it will notify the VEP Executive Secretariat as soon as is practicable and provide its recommendation to either disseminate or restrict the vulnerability. The submission will include, at a minimum, information describing the vulnerability, identification of the vulnerable products or systems, and a recommendation on dissemination of the vulnerability information.

5.2.2. Notification

The VEP Executive Secretariat will notify all VEP POCs within one business day of acknowledging the submission and request that participants respond if they have an equity at stake.

5.2.3. Equity and Discussions

An agency that claims an equity must indicate whether it concurs with the recommendation to disseminate or restrict within 5 business days.

The primary purpose of sharing among agencies is to gain consensus on recommendations for the ERB. If an agency does not concur with a recommendation to disseminate or restrict, one or more SMEs from the submitting agency will hold discussions with the non-concurring agency or agencies and the VEP Executive Secretariat within 7 business days to reach consensus. If no consensus is reached, the participants will provide options for the ERB.

5.2.4. Determination to Disseminate or Restrict

Decisions whether to disclose or restrict a vulnerability will be made quickly, in full consultation with all concerned agencies, and in the overall best interest of USG missions of cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection.

To the extent possible and practical, determinations to disclose or restrict will be based on repeatable techniques or methodologies that enable benefits and risks to be objectively evaluated by VEP participants. This process employs techniques that include assessment factors such as prevalence, reliance, and severity in accordance with the equity considerations in Annex B.

ERB determinations for follow-on actions and next steps should be reached in a timely fashion. When there is consensus among those agencies that claimed an equity, the timeline will be shortened.

It is the intent of VEP participants that ERB determinations be made by consensus. If the ERB members cannot reach consensus, they will vote on a preliminary determination. If an agency with an equity

disputes the preliminary determination of the ERB, that participant may, by providing notice to the VEP Executive Secretariat, elect to contest the preliminary determination in accordance with Section 5.2.6. If no agency contests a preliminary determination, it will be treated as a final determination.

5.2.5. Handling and Follow-on Actions

If vulnerability information is released, dissemination will be made in the most expeditious manner and when possible within 7 business days. Disclosure of vulnerabilities submitted for equity review will be conducted according to agreed-upon guidelines that are consistently and responsibly followed by all members. The submitting agency is presumed to be most knowledgeable about the vulnerability and, as such, will be responsible for disseminating vulnerability information to the vendor. If the submitting agency so chooses, it may elect to delegate dissemination responsibility to another agency on its behalf. The releasing agency will promptly provide an information copy of dissemination information to the VEP Executive Secretariat for record keeping. Additionally, the releasing agency is expected to follow-up so the ERB can determine whether the vendor's action meets USG requirements. If the vendor chooses not to address a vulnerability, or is not acting with urgency consistent with the risk of the vulnerability, the releasing agency will notify the VEP Executive Secretariat, and the USG may take other mitigation steps.

If vulnerability information will be restricted, the submission will be reassessed annually by the ERB until dissemination is accomplished, the vulnerability is publicly known, or the vulnerability is otherwise mitigated. Submitting agencies are also responsible for engaging with other VEP members to address various mitigation options, regardless of a decision to disseminate or restrict, which may include engaging a broader stakeholder community beyond the USG.

5.2.6. Contested Preliminary Determinations

Disputes arising from the VEP, including any challenges by an agency to a preliminary determination by the ERB, will be resolved using the process described in National Security Presidential Memorandum (NSPM)-4, of April 4, 2017, *Organization of the National Security Council, the Homeland Security Council, and Subcommittees*. If an agency participating in the VEP wishes to contest a preliminary determination, it will notify the VEP Executive Secretariat of its intent to do so and the basis for its decision within 5 business days of the ERB's preliminary determination. The VEP Executive Secretariat will notify the VEP Director. Disclosure of any vulnerabilities preliminary determined to be disclosable will be delayed until the matter has been resolved. If a policy concern arises within the Executive Office of the President over an ERB preliminary determination, the VEP Director will arrange for further discussion with the ERB.

5.3. Considerations

Making consistent, informed determinations and understanding risk is critical to ensure an equitable review of vulnerability information. Consideration of defensive, military, intelligence and operational,

commercial, international relationships, and law enforcement equities is required when making vulnerability equities determinations.

All USG agencies will appropriately safeguard information concerning vulnerabilities identified by other entities, to include private businesses, researchers, and foreign governments. As appropriate, the USG will work with such entities to encourage them to disclose vulnerabilities consistent with international standards and/or current best practices, and/or take additional actions to reduce risk.

The USG's decision to disclose or restrict vulnerability information could be subject to restrictions by foreign or private sector partners of the USG, such as Non-Disclosure Agreements, Memoranda of Understanding, or other agreements that constrain USG options for disclosing vulnerability information.

If a vulnerability is found in GOTS equipment or systems that were 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 practical. NSA will assume responsibility for this vulnerability and submit it formally through the VEP Executive Secretariat.

When an agency discovers ongoing malicious cyber activity that exploits a vulnerability that is subject to a prior and ongoing decision to restrict, the USG entity will immediately report this information to the VEP Executive Secretariat. In such circumstances, the vulnerabilities equities discussion will begin no later than the business day following notification to the VEP Executive Secretariat, and participants will expeditiously reach consensus on disclosure or appropriate mitigation actions, or raise issues to the ERB.

5.4. Exceptions

There are specific, limited categories of vulnerabilities that may be excluded from VEP review.

The United States Government's decision to disclose or restrict vulnerability information could be subject to restrictions by partner agreements and sensitive operations. Vulnerabilities that fall within these categories will be cataloged by the originating Department/Agency internally and reported directly to the Chair of the ERB. The details of these categories are outlined in Annex C, which is classified. Quantities of excepted vulnerabilities from each department and agency will be provided in ERB meetings to all members.

Vulnerabilities identified through security researcher activity and incident response that are intended to be disclosed in a rapid fashion will not be subject to adjudication by the VEP.

The following will not be considered to be part of the vulnerability evaluation process:

- Misconfiguration or poor configuration of a device that sacrifices security in lieu of availability, ease of use or operational resiliency.
- Misuse of available device features that enables non-standard operation.
- Misuse of engineering and configuration tools, techniques and scripts that increase/decrease functionality of the device for possible nefarious operations.
- Stating/discovering that a device/system has no inherent security features by design.

Annex A
Definitions

The following terms are defined to clarify their use in the Vulnerability Equities Policy and Process document.

Commercial off-the-shelf (COTS)	A software and/or hardware product that is freely available or commercially ready-made and available for sale, lease, or license to the general public.
Equities Review Board (ERB)	Primary forum for interagency deliberation and determinations concerning the VEP, with senior level representation from agencies with authorities and responsibilities in national defense, homeland security, law enforcement, and national intelligence. Core membership is coordinated through the NSPM-4 process. Other agencies may be invited to participate when demonstrating responsibility for or identifying equity in a vulnerability submission under deliberation.
Exploit	A tool, code, or action designed to take advantage of a vulnerability and execute unexpected or unintended behavior, or impact confidentiality, integrity, or availability of information.
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
Industrial Control System (ICS)	A term that encompasses several types of control systems to include SCADA 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.
Newly Discovered	After February 16, 2010, the effective date of the initial Vulnerabilities Equities Process, when the USG discovers a zero-day vulnerability or new zero-day vulnerability information, it will be considered newly discovered.

	This definition does NOT preclude entry of vulnerability information discovered prior to February 16, 2010.
Publicly known	A vulnerability is considered publicly known if the vendor is aware of its existence and/or vulnerability information can be found in the public domain (e.g., published documentation, Internet, trade journals).
Vulnerability	A weakness in an information system or its components (e.g., system security procedures, hardware design, internal controls) that could be exploited or impact confidentiality, integrity, or availability of information.
Zero-Day Vulnerability	A type of vulnerability that is unknown to the vendor, exploitable, and not publicly known.

Annex B
Equity Considerations

The list below enumerates core considerations the Vulnerability Equities Process and Policy will use when evaluating vulnerability equities. These considerations have been selected to help decision-makers weigh the benefits to U.S. national security and national interest when deciding whether to disclose or restrict knowledge of an identified vulnerability. Evaluations will not be limited to applying only these considerations, but these represent general concerns, which should apply to all vulnerability equity decisions. The questions are phrased assuming that the USG has detailed non-public knowledge of a vulnerability in some commercially available product, component, system, or program (the 'product') sold, distributed, or supplied by some private sector party (the 'vendor').

Note that in all of the discussions about product usage, intelligence and law enforcement value, mitigations, and other areas, care should be taken to consider both current and near-term future conditions.

Part 1 – Defensive Equity Considerations

1.A. Threat Considerations

- Where is the product used? How widely is it used?
- How broad is the range of products or versions affected?
- Are threat actors likely to exploit this vulnerability, if it were known to them?

1.B. Vulnerability Considerations

- What access must a threat actor possess to exploit this vulnerability?
- Is exploitation of this vulnerability alone sufficient to cause harm?
- How likely is it that threat actors will discover or acquire knowledge of this vulnerability?

1.C. Impact Considerations

- How much do users rely on the security of the product?
- How severe is the vulnerability? What are the potential consequences of exploitation of this vulnerability?
- What access or benefit does a threat actor gain by exploiting this vulnerability?
- What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
- Will enough USG information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?

1.D. Mitigation Considerations

- Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
- Are impacts of this vulnerability mitigated by existing best-practice guidance, standard configurations, or security practices?
- If the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it?
- If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released?
- Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

Part 2 – Intelligence, Law Enforcement, and Operational Equity Considerations

2.A. Operational Value Considerations

- Can this vulnerability be exploited to support intelligence collection, cyber operations, or law enforcement evidence collection?
- What is the demonstrated value of this vulnerability for intelligence collection, cyber operations, and/or law enforcement evidence collection?
- What is its potential (future) value?
- What is the operational effectiveness of this vulnerability?

2.B. Operational Impact Considerations

- Does exploitation of this vulnerability provide specialized operational value against cyber threat actors or their operations? Against high-priority National Intelligence Priorities Framework (NIPF) or military targets? For protection of warfighters or civilians?
- Do alternative means exist to realize the operational benefits of exploiting this vulnerability?
- Would disclosing this vulnerability reveal any intelligence sources or methods?

Part 3 – Commercial Equity Considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?

Part 4 – International Partnership Equity Considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?