Fact Sheet

FACT SHEET: Vulnerabilities Equities Process

The newly released Vulnerabilities Equities Process (VEP) Charter spells out how the Federal Government will handle the process that determines whether the Government will notify a private company about a cybersecurity flaw in its product or service or refrain from disclosing the flaw so it can be used for operational or intelligence-gathering purposes.

Today, executive departments and agencies released a new charter governing the Vulnerability Equities Process (VEP). The charter builds on lessons learned and improves the Federal Government's implementation of this important process, and its release marks a significant increase in transparency about this topic.

Cyber threats are on the rise, and the Administration must act to address them. During the President Trump's campaign, he promised to strengthen America's cybersecurity capabilities and secure America from cyber threats. The release of this Charter and adherence to the rigor it demands follows through on that commitment to the American people. The Administration is committed to a free, open, interoperable global internet and understands that vulnerabilities in technologies underpinning the Internet threaten both security and liberty. America built the internet and shared it with the world; now, we must make sure to preserve cyberspace for future generations by promoting responsible cyber behavior. The VEP process is an example of our commitment to accountable behavior online.

In the course of carrying out its missions, the Federal Government may itself identify vulnerabilities that cyber actors could exploit. In the vast majority of these cases, responsibly disclosing a newly discovered vulnerability is in the national interest. Such vulnerabilities will be disclosed through a process similar to that used when the Government, or other vulnerability numbering authorities, learn of vulnerabilities from independent security researchers. Vulnerabilities can have significant economic, privacy, and national security implications when exploited, and our dependency on cyberspace puts us at heightened risk. At times, however, we might compromise criminal investigations or lose crucial intelligence opportunities through their publication.

In recognition of these occasionally competing considerations, new and not publicly known cyber vulnerabilities are reviewed by multiple departments and agencies to determine whether they should be disclosed to the public using what is known as the VEP. At its most basic, the VEP balances whether to disclose vulnerability information in the expectation that the vulnerability will be patched, or temporarily restrict the knowledge of the vulnerability to the Federal Government so it can be used for national security or law enforcement purposes.

The Federal Government has an important responsibility to closely guard sensitive information and protect vulnerabilities. Any unauthorized disclosures damage both our reputation and our ability to carry out intelligence missions. These consequences have only heightened our interest and awareness in ensuring we conduct the VEP in a manner that can withstand a high degree of scrutiny and oversight – a consideration that does not often encumber our adversaries. The United States is a world leader when it comes to this topic, and no other nation in the world has created and run a process as advanced and meticulous as ours. While our processes may not be infallible, they are intended to apply rigor in a mission area that is key to our national security.

As we have made progress on the implementation of the VEP, the United States has been faced with managing increasingly significant vulnerabilities affecting both the private sector and the Federal

Government. Executive departments and agencies have applied the lessons learned from these instances to hone the Federal Government's approach when determining whether to disclose a vulnerability. We have also heard from our stakeholders that they need more transparency into this important process. We have spent the last few months reviewing our existing practices so we can implement improvements and take steps to make public key details about the VEP.

These efforts affirmed many aspects of the existing process and ensured that we will continue to adhere to a rigorous standard. At a high level, we consider four major groups of equities. These core considerations, which have now been explicitly incorporated in the VEP, will help to standardize the process by which decision-makers weigh the benefit to national security and the national interest when deciding whether to disclose or restrict knowledge of a vulnerability. Evaluations are not limited to applying only these considerations, but these represent our general concerns.

1. Defensive Equity Considerations

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?

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?

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?

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?

2. Intelligence, Law Enforcement, and Operational Equity Considerations

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?

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?

3. Commercial Equity Considerations

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

4. International Partnership Equity Considerations

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

Vulnerability management requires sophisticated engagement to ensure protection of our people, the safeguarding of critical infrastructure, and the defense of important commercial and national security interests. The new VEP Charter balances those interests in a way that is repeatable and defensible, and its publication will bolster the confidence of the American people as we continue to carry out this important mission.