

“Early Stage” Coordinated Vulnerability Disclosure Template Version 1.1

NTIA Safety Working Group
December 15, 2016

Executive Summary

Collaboration between technology providers and security researchers is part of good information security. As security researchers and organizations’ technology, those organizations benefit from working with the researcher to understand and mitigate collaboration across the digital ecosystem, the National Telecommunications Administration (NTIA) convened a multistakeholder process to address security researcher disclosure.

This document reflects the work of the “Safety” working group. It describes steps an organization can take to improve collaboration. It is open, transparent fashion, with diverse participation from the security community. Much of the discussion targeted the potential for harm directly impacts public safety or causes (e.g., medical devices), but the lessons are easily adaptable by software or systems.

In this report, we discuss why security disclosure is important for industries that are becoming more and more dependent on present a template disclosure policy, explain the different sectors for “Acme Corp.” At the end of this document, we walk through how you should consider when developing a security disclosure policy.

¹The Working Group is soliciting public comment on this draft, and interested parties are encouraged to provide feedback to: afriedman@ntia.doc.gov to pass along to the working group.

²More information on NTIA’s open Multistakeholder Process to Promote Transparency and Accountability in the Disclosure of Vulnerabilities is available at <https://www.ntia.doc.gov/other--publication/2016/multistakeholder--process--cyber-vulnerabilities>.

Introduction: Disclosure and Safety

Safety-critical systems are increasingly dependent on software, subject to software security issues. Coordinated vulnerability attention into improving the safety and security of systems and population. Compared with traditional IT systems, manufacturing a higher consequence of failure and relatively less experienced trust, high collaboration interactions come from understanding perspectives.

We define “safety-critical industries” as those in which humans – for example, an automobile, an embedded medical insulin pump), or carbon monoxide detectors. Compared differences that must be appreciated and³ accounted for. These than just disclosure policies and actions (by multiple stakeholders); consider how design choices will limit or grant capabilities vulnerabilities.

- **Consequences:** When software is a dependency for safety consequences of security failure may manifest in direct of life. Impacts from wide-scale harm can shatter and can damage trust in government and its role safety and regulation.
- **Adversaries:** Different adversaries have different goals, capabilities. While some adversaries may be detected impacting systems, others may seek these systems may wish to inflict harm, and criminal groups may demand ransoms.
- **Composition:** Some components in Internet of Things are not found in typical IT environments. Elements such as controllers, low power chips, embedded controllers, limited capabilities available to the manufacturer in design and responsibility.
- **Economics:** Components for safety systems may require protect and have a very low cost of goods, Security capabilities for million-dollar data centers are microchips, for example.
- **Context and Environment:** Safety-critical systems often exist in environmental, physical, network, immediacy/real-time, and legal

³I Am the Cavalry. “6 Differences in Internet of Things and <https://www.iamthecavalry.org/iotdifferences/>

instance, a pacemaker is implanted in a human immediately, has no bolt-on security measures, and carries requirements.

- Timescales: Timescales for design, development, implementation, retirement are often measured in decades. Response time because of composition, context, and environment. Safety be with us for 10, 20, 40, or more years.

Vulnerability disclosure and remediation in cyber safety context due haste and due care. Researchers may be more vulnerability has not been (or cannot be) fixed. On the consequence failures may motivate action. Remediation urge trust; at the same time, validation and verification avoid increase risk. Decisions considered insecure for a web implanted medical device. Any hard deadline for disclosure or long and too short to safely address security vulnerabilities

We believe Coordinated Vulnerability Disclosure is especially safety-critical industries. [DMCA](#), [which exemptions](#) significant to security research on cars and medical devices, went softened fear of legal concerns, higher numbers of researcher vulnerability research and disclosure in safety-critical industries. should understand how the security research community themselves with a flexible set of tools to successfully

Disclosure Policy: The First Steps

Stakeholders representing a range of interests in this community approach that starts small to build experience, confidence contemplating their first steps into Coordinated Vulnerability and references from multiple sources available to consult journey has taken many years for even the most

What follows is a simple framing of what an “early might look like. Below, we present a template of what disclosure policy might look like and then highlight some policy. We also present a sample disclosure policy.

⁴ US Copyright Office. “Exemption to Prohibition on Circumvention of Technologies” 80 FR 65944 (2015). Available at: <https://www.federalregister.gov/2015/07/27/2015-14712/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control>

There are many resources on how to think about vulnerability, including ISO/IEC Standards ⁵ 29147 and 30111, and information produced by stakeholders in the NTIA process may be Disclosure Attitudes and Actions: ⁶ A Research Report” background disclosure, and “Guidelines and Practices for Multi-party Vulnerability Coordination” ⁷ for organizations facing more complex disclosure challenges.

⁵ ISO/IEC 29147 “Vulnerability Disclosure” (2014) http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231 standard is publicly available at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/> “Vulnerability Handling Processes” (2013) can be found at http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231

⁶ “Vulnerability Disclosure Attitudes and Actions: A Research Report” (2016) https://www.ntia.doc.gov/files/ntia/publications/2016_NTIA_A_A_vulnerability_insights_report.pdf

⁷ “Guidelines and Practices for Multi-party Vulnerability Coordination” (2016). This <https://www.first.org/global/sigs/vulnerability--coordination/multiparty>

Template Disclosure Policy

The first step an organization should take is to develop a policy. We urge the creation/use of a simple, short, readable page. Many organizations, including automakers and already done this, leveraging the template below.

Brand Promise

Objective: To demonstrate a clear, good faith commitment to stakeholders potentially impacted by security vulnerabilities.

Audience: Customers and the market

Tone: Committed, concerned, and open. For instance, "The is important to us..."

Content: Assure customers and the market that safety and work has already been done as well as future commitment. reporter can serve as outreach and can build trust up this program to give security researchers a point of research findings, which can then be remediated in a

Initial Program and Scope

Objective: To outline which systems and capabilities are "fair" initial program, which will evolve as capacity and confidence

Audience: Vulnerability finders and reporters

Tone: Set a reasonable initial phase to build capacity

Content: Declaration of explicit and/or implicit scope, and scope. Explicit scope sets an expectation for what reports, such as models/years and versions as well as duration, recognition and/or reward, allows a degree of throttling of and can be expanded over time as well. Optionally, unintended harm from good faith research, though a

"We Will Not Take Legal Action If..."

Objective: To assure that vulnerability finders and reporters of their good faith acts.

Audience: Vulnerability finders and reporters

Tone: Non-threatening, inviting, and reasonable, using language without a legal background or representation. Affirmative than prohibitive, with some key exceptions such as

Content: Clear, unambiguous statements that guide researcher should tell researchers what activities will and won't result

evergreen and is very unlikely to change. This section from deviating.

Other Considerations: This section should contain legal priorities, which will come later. Parties should account national/federal laws.

Communication Mechanisms and Process

Objective: To clearly identify communication mechanisms and reasonable timeframe.

Audience: Vulnerability finders and reporters

Tone: Reasonable for the initial information exchange

Content: Define a mechanism for submission and reporting, (such as a PGP encryption key) and requirements for communication from a legal posture). Many organizations prefer a secure set expectations for when the researcher can expect to submit and how future engagement/communication will take outline conflict resolution mechanisms and roles and responsibilities.

Nonbinding Submission Preferences and Prioritizations

Objective: To set expectations based on priorities and submission legal objection or restriction.

Audience: Vulnerability finders and reporters

Tone: How bugs will be triaged/prioritized

Content: This section is a living document that sets typically maintained by the support and engineering team. vulnerabilities, reporting style (crash dumps, CVSS scoring, Too many preferences can set the wrong tone or make This section also sets expectations to the researcher communication considered important or not.

Versioning

Objective: To track the evolution of the policy.

Audience: Vulnerability finders and reporters

Tone: Organized to help the researcher understand adjustments to the policy.

Content: This optional section can help the reader understand how it might evolve in the future. See "Changing the

Sample Vulnerability Disclosure Policy Template

ACME Corp.

Brand Promise

ACME Corp., the leading manufacturer of embedded software ensuring the safety and security of our customers. Toward our policy for accepting vulnerability reports in our products. partnership with the security community, and we recognize that is important in continuing to ensure safety and security

We have developed this policy to both reflect our responsibility to good-faith security researchers that are prov

Initial Program and Scope

Initial

Scope

ACME's Vulnerability Disclosure Program initially covers the

- ACME Widgetsoft 3.1
- ACME Widget Module A
- ACME Widget Module B
- ACME Widget Controller
- ACME Widget Ethernet Gateway Module

While ACME develops a number of other products, we ask vulnerability reports only for the stated product list. We build capacity and experience with this process.

Researchers who submit a vulnerability report to us the submission has been accepted and validated by our prod

We Will Not Take Legal

Legal

Posture

ACME Corp will not engage in legal action against indiv through our Vulnerability Reporting Form. We openly accept ACME products. We agree not to pursue legal action again

- Engage in testing of systems/research without harming
- Engage in vulnerability testing within the scope of and avoid testing against [ex. website].
- Test on products without affecting customers, or receive customers before engaging in vulnerability testing against
- Adhere to the laws of their location and the local laws that would only result in a claim by ACM

- acceptable as ACME is authorizing the activity (reverse protective measures) to improve its system. Refrain from disclosing vulnerability details to the public timeframe expires.

Communication Mechanisms and Process

How to Submit a Vulnerability
To submit a vulnerability report to ACME's Product Security form <[link to vulnerability reporting form](#)>

Nonbinding Submission Preferences and Process

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions:

What we would like to see from you:

- Well-written reports in English will have a higher priority.
- Reports that include proof-of-concept code or other evidence will be prioritized.
- Reports that include only crash dumps or other low-quality evidence will have a lower priority.
- Reports that include products not on the initial scope will be prioritized.
- Please include how you found the bug, the impact, and any other relevant information.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline, and communicate possible about the remediation timeline as well as on how we can help.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed.
- Credit after the vulnerability has been validated and resolved.

If we are unable to resolve communication issues or other concerns, we will refer you to a neutral third party (such as CERT/CC, ICS-CERT, or others) for determining how best to handle the vulnerability.

Versioning

This document Version 1.1 was created 15--December--2016. [We update every 90 days.] Any updates will be noted below in the document.

⁸For an example of a secure web form, see [cert.org's Vulnerability Reporting Form](https://vulcoord.cert.org/VulReport/form).

Issues to Consider in Writing a Disclosure

Defining Vulnerability Disclosure Program Scope

Any newly implemented vulnerability disclosure program may unanticipated volume of submissions. In the early stage, explicit or implicit scoping in the disclosure policy. This the specific type of disclosure items the company is prep capacity and experience.

For example, submissions could be explicitly scoped by limit

- Only specified product model years
- Only select product make/model/year
- Only particular types of vulnerabilities

Implicit scoping may be influenced by the type, stru awarded to researchers, if any incentives are used at particular area for finding security issues is one way of scope may come from the reward structure. A Coordinat with no reward program is likely to attract altruistic indiv their findings with the company, but are not looking for a and/or a reward to the program could expand the scop Rewards such as providing recognition on a wall of fam and/or branded merchandise attracts some researchers to rewards will attract researchers as well, and will be less limit the response from the research community.

Researchers are motivated to understand security flaws desire to solve an interesting problem to a desire illustrates some of the diverse types of motivations rese narrowing the scope and/or having no financial incentive for limiting the number of reported vulnerabilities; and attracting rese patience and/or less motivation to disclose during conferenc deadlines), the dates of which could conflict with the

Table 1 -- Diverse Motivations of Security Researchers

Researchers	Motivation	Description
Protect		Wants to make the world a safer place by addressing realities affecting safety.
Puzzle		Tinkerers, curiosity, hobbyists. Driven by 'Hacking for the good'
Prestige/Pride		Recognition, making a name, conference presentations
Profit/Professional		Seeking monetary reward and/or making a living
Politics/Patriotism/Protest		Ideological or principled. E.g. Civil liberties, anti-causes or organizations.

In summary, an organization can use explicit and implicit scope to implement its disclosure program. As the organization's experience through responses to vulnerability disclosures, its capabilities, explicit and implicit, mature, its response capabilities, explicit and implicit, may be relaxed so that more useful disclosures may be made. Programs should be prepared for such a contingency. Well-intentioned finders who are aware of a vulnerability may still be able to exploit the current policy.

Changing the Disclosure Policy

As with any policy, at some point, it may need to be changed. Changing the disclosure policy is that it can make things difficult for vendors to track, or can cause researchers to change their behavior. As such, we recommend minimizing changes if possible. Legal protections offered to researchers should not change.

Given that policies may change, some strategies to maintain consistency are:

- Be transparent - explain why the disclosure policy is changing
- Accept feedback on changes / listen to the community
- Explicit duration of any given policy: This policy will last for X months
- Include version control
 - For any change made; archive prior versions (confer with the organization's site)

⁹ | Am The Cavalry. "5 Motivations of Security Researchers." Available

- Avoid abrupt or erratic changes in the policy, and time periods
- Consider allowing researchers to enroll, and become gran version
 - This puts a lot of responsibility on to the rese which policy version is being used
 - [Light version: have a feed or email list for
- Include explicit caveats about how the policy will
 - This may result in a very long and com
 - Black lists will invariably grow
 - Potential solutions: white listing (allowed) over black part
- Declare certain parts of the policy immutable, promises
 - Have a baseline - everything above this point
 - Baseline = white list (allowed)
 - Consider tying in with brand promise
 - Should reflect high level goals of prog rather than technical approaches
 - Changes to white list (adding or removing) accompanied with an explanation for the char
 - Here is the section that we may change - esta
 - Changing = black list
 - May be used to throttle common or “low
 - May change as a result of enhanced security
 - May be used to shift the focus to the
 - Can encourage researchers to check back, and the research against (in good faith) to grandfath
 - Can subscribe to an RSS feed of updates

Resolving these issues will help inspire confidence amo success of the policy.

Restrictions on Disclosure

Researchers do not create vulnerabilities. The fact that one rese existence does not guarantee that another will not find it may have reasons to want to disclose the vulnerability motivations discussed above. A managed disclosure situation is pref control. Vendors may want to express preferences on vulnerabilities. A few options are:

Do not publicly disclose:

1. Until it is fixed

2. Until a particular timeframe after first submission
3. Until after giving the organization X days of notice
4. Mutually agreed-upon (or negotiated) timeline (as discussed) technologies or sectors may have different timelines) the process with the disclosing party. (Note: Communication researcher is critical in this part of the process because researcher will know progress is occurring and the organization seriously)

There are strong pros and cons for denying researchers an organization states that “no disclosures can happen until be less risk of exploitation, but there may also be risk participate. What if they fear a vendor “sitting” on a

- What if the fix takes 5 years?
- Some researchers may expect very fast turnarounds industries can’t turn on a dime.

Because reasonable people can disagree on the method and also be prudent to have a defined path of escalation appropriate guidance/participation from the regulator of jurisdiction governments (e.g. US FDA or NHTSA - and US DHS--ICS-- medical device, the FDA may be best poised to determine ecosystem - as well as the optimal safety communication strategy