"Early Stage" Coordinated Vulnerability Disclosure Temp
Version [1]1.1

NTIA Safety Working Group

December 15, 2016

Executive Summary

Collaboration between technology providers and security researcher part of good information security. As security researchers organizations' technology, those organizations benefit from working with the researcher to understand and mitigate collaboration across the digital ecosystem, the National Tele Administration (NTIA) convened a multistakeholder process to around security researcher[2] disclosure.

This document reflects the work of the "Safety" working grou steps an organization can take to improve collaboration. It open, transparent fashion, with diverse participation from security community. Much of the discussion targeted the potential for harm directly impacts public safety or caus or medical devices), but the lessons are easily adaptable by maintains its own software or systems.

In this report, we discuss why security disclosure is impo industries that are becoming more and more dependent on present a template disclosure policy, explain the different sect for "Acme Corp." At the end of this document, we walk should consider when developing a security disclosure polic

[1] The Working Group is soliciting public comment on this draft, and inter feedback to: afriedman@ntia.doc.gov to pass along to the working group.

[2] More information on NTIA's open Multistakeholder Process to Promote process is available at https://www.ntia.doc.gov/other--publication/2016/multistakeholder--process--cy 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, manufactu a higher consequence of failure and relatively less experienc trust, high collaboration interactions come from understan perspectives.

We define "safety--critical industries" as those in which humans – for example, an automobile, an embedded med insulin pump), or carbon monoxide detectors. Compared differences that must be appreciated and accounted for.[3] The than just disclosure policies and actions (by multiple stakeholders); consider how design choices will limit or grant capa vulnerabilities.

- Consequences: When software is a dependency for safe consequences of security failure may manifest in direc of life. Impacts from wide--scale harm can shatter and can damage trust in government and its role safe and regulation.

- Adversaries: Different adversaries have different goals, capabilities. While some adversaries may be dete impacting systems, others may seek these systems may wish to inflict harm, and criminal groups may ransoms.

- Composition: Some components in Internet of Things are not found in typical IT environments. Elements such controllers, low power chips, embedded controllers, limit capabilities available to the manufacturer in design and resp

- 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 exis environmental, physical, network, immediacy/real--time, and legal

[3] I 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 carr 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 cont 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[4], which exemptions to security research on cars and medical devices, went softened fear of legal concerns, higher numbers of researche 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 com 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 wha disclosure policy might look like and then highlight som 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 27212/exemption--to--prohibition--on--circumvention--of--copyright--protection--systems--for--access--control

There are many resources on how to think about vuln
including ISO/IEC Standards [5] 29147 and 30111. For more information, two ot
produced by stakeholders in the NTIA process may be
Disclosure Attitudes and Actions: A Research Report" [6] with background
disclosure, and "Guidelines and Practices for Multi--party Vulnerabil [7] for
organizations facing more complex disclosure challenges.

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

[6] "Vulnerability Disclosure Attitudes and Actions: A Research Report" (201
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 deve
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 commitme
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 commitme
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 capa
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 dura
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 lang
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 resu

evergreen and is very unlikely to change. This section from deviating.
Other Considerations: This section should contain lega priorities, which will come later. Parties should account national/federal laws.

Communication Mechanisms and Process

Objective: To clearly identify communication mechanisms and reas 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 com from a legal posture). Many organizations prefer a secu set expectations for when the researcher can expect to submission and how future engagement/communication will take outline conflict resolution mechanisms and roles and responsibi

Nonbinding Submission Preferences and Prioritizations

Objective: To set expectations based on priorities and submissio 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 mak This section also sets expectations to the researcher com 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 unde how it might evolve in the future. See “Changing the

Sample Vulnerability Disclosure Policy Templa

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 proc

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 agai

- 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 loca
  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 publ timeframe expires.

Communication Mechanisms and Pr

How to Submit a Vulnerability

To submit a vulnerability report to ACME's Product Secu form <link to vulnerability[8] reporting form>

Nonbinding Submission Preferences and F

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage subr

What we would like to see from you:
- Well--written reports in English will have a higher
- Reports that include proof--of--concept code equip us
- Reports that include only crash dumps or other lower priority.
- Reports that include products not on the initial scope
- Please include how you found the bug, the impa
- Please include any plans or intentions for public disc

What you can expect from us:
- A timely response to your email (within 2 busi
- After triage, we will send an expected timeline, and com possible about the remediation timeline as well as on extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed
- Credit after the vulnerability has been validated and

If we are unable to resolve communication issues or othe neutral third party (such as CERT/CC ,ICS--CERT, or determining how best to handle the vulnerability.

Versioning

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

[8] For an example of a secure web form, see cert.org's Vulnerability 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 Coordinate 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[9] of Security Researchers

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

In summary, an organization can use explicit and implicit scop capacity to implement its disclosure program. As the organizati experience through responses to vulnerability disclosures, it With maturation of the organizational response capabilities, expl limitations may be relaxed so that more useful disclosure vulnerabilities that fall outside the program scope may still and response. Programs should be prepared for such a cont well--intentioned finders who are aware of a vulnerability the current policy.

Changing the Disclosure Policy

As with any policy, at some point, it may nee changing the disclosure policy is that it can make things difficult for vendors to track, or can cause researchers As such, we recommend minimizing changes if possible. legal protections offered to researchers should not change maintained.

Given that policies may change, some strategies to maintain

- Be transparent – explain why the disclosure policy
  - Accept feedback on changes / listen to the com
- Explicit duration of any given policy: This policy
- Include version control
  - For any change made; archive prior versions (con the organization's site)

[9] I 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 blac
- Declare certain parts of the policy immutable, part 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 grandfathe
    - 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 noti
4. Mutually agreed--upon (or negotiated) timeline (as discussed
   technologies or sectors may have different timelines)
   the process with the disclosing party. (Note: Communic
   researcher is critical in this part of the process beca
   researcher will know progress is occurring and the organizati
   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 dete
ecosystem – as well as the optimal safety communication strat