This document was compiled in real time from the stakeholder discussion on working group presentations at the November 7, 2016 multistakeholder meeting on Collaboration on Vulnerability Research Disclosure. No attempts to edit or organize the raw notes have been made.

http://www.ntia.doc.gov/other-publication/2015/multistakeholder-processcybersecurity-vulnerabilities

---

Q&A for presentations

Safety WG

- The template can apply more broadly, beyond the Safety WG scope
- Discussion regarding whether a broader context should be mentioned in the introduction, as many other devices can have a physical safety aspect
- Researchers can be acting in good faith and still cause an issue re vuln disclosure (e.g., ransomware targeting hospitals, derived from shared library disclosure)
- Template: geared toward showing you are operating in good faith
- Next steps: External resources/links will be included in the draft (ISO standard); Add back in 5Ps

Multiparty WG

- Considering releasing the draft for public comment to ensure input from stakeholder groups that may not have been participating actively
- What can make it easier to do cross-sector impact assessment?
  - E.g., an FDA master database of products that use open source software – if product makers go out of business, would still have information on software if vulns are revealed later
- Discussed a directory of contacts at organizations for vuln disclosure
  - POCs for org CSIRTs
  - Hacker 1 has dynamic directory

Awareness & Adoption WG

- How to address legal fears chilling research?
  - Adoption issue
- Who should we partner with to drive better adoption?

    - Government agencies currently supporting message: FDA; NHTSA best practices for vehicles includes vulnerability reporting policy; FTC talking about vuln disclosure being reasonable for vendors;
    - Government agencies not yet supporting message
    - Who could do more? NIST pointing people more aggressively to ISOs;
    - Industry groups or associations? How do we engage them?
- How do we get those already following best practices to share experiences with others?
    - Activism can occur in groups that work closely with vendors, build more collaborative environment
    - Good when companies want to compete on security, how to provide an environment for that
- Civil nuclear has a sharing issue. One vendor shared information on a cyber attack. You have to find the single org that will jump first. Venue may be ISACs and ISAOs. Each group seems to have a lead organization with varying levels of maturity.
- Medical device makers – many launching vuln disc programs. Opportunities for more sharing?
    - Champions among manufacturers. How can agencies showcase and applaud that behavior and drive further adoption? Partnering with trade organizations, etc.
    - Agencies want to know: what are the actual impediments preventing manufacturers from establishing disclosure policies?
    - Health care sector has been faced with serious concerns for providers and stakeholders, possibilities of adversarial consequences.
- Stories of what works re sharing best practices – it works best with hands-on guidance. Go beyond theoretical and include the practical.
- Refocus on scenarios in segments of business or different sizes. Make it somewhat anonymous. Case studies.
    - Concrete examples are powerful
    - Handshake site, like Facebook platform that provides case studies, announcements about examples for the health sector, best practices, not under the regulator. Creates dialogue across different stakeholders.
- Awareness: getting outside the echo chamber; we try to find an industry group where security is not the main focus.
- Diversify vocabulary: people listen quickly when you talk about risk management and FTC settlements. In info sharing commty, this is a risk mgmt. issue. Adopt relevant vocab for groups we are targeting
- Communicate <u>why</u> companies should adopt best practices
- List of FAQs? Or Should Be Asked Qs (by those new to the realm)?
    - Centralized FAQ does exist for things people should ask in initial disclosure situation
    - The FAQ that is needed is on multi-party disclosure

    - Collect list of relevant resources; Google doc for questions that come up frequently
        - Could help meaningfully identify the true edge cases
- Address lawyers directly – talk at law conferences, bring together research and legal community. Not so much legal researchers but in-house counsel. Appropriate venues? Association of Corporate Counsel, GC Summit, other venues. Key is raising awareness among counsel.
    - Lawyers often focus on fraud. Lawyers may need to better understand the difference between a vuln disc and fraud.
- State/local govts and law enforcement could benefit from this process. LE often hostile to concept of security researchers. Apply knowledge from more sophisticated cyber crime world to state/local
- This is an enterprise risk management issue, need to get to corporate directors. How to get Boards to care?
    - Idea of being more insurable or better corporate citizen with policies like this in place
    - Brand reputation is important and relevant – e.g., data breach hurts your brand; focus on those who manage the brand's reputation
    - Reputation issue also relevant to underwriters. Cyberinsurance is growing fast. How to link into that discussion?
    - Risk-Based Security – has lots of data
    - Tie it into principle of resilience
    - Relationship to procurement – but beware of unintended consequences e.g., Sidekick hack
    - Promulgate best practices, risk of drawing hard and fast rules; how to determine what standards should look like
    - Value in doing case studies of the failed pieces in organization change (not the disclosure failures specifically).
- Partners: Business to business
- Fintech:
- Open source: Communication and timing of disclosures, org that has a fix for its own subset shouldn't be held back by other orgs that are working it too; Protocol level vuln – closed and open source implementations; the right to protect your main user base without putting the entire affected user base in harm's way. What is the balance?
- Industry groups/trade assoc: Consumer Technology Association, National Retail Federation, Better Business Bureau
- Progress made within past yr to 18 mo (eg NHTSA draft proposal):

How to move forward

- Proposal: Come to consensus and polish documents currently in draft while continuing to work on the awareness and adoption product.
    - Make sure there is no conflict between the two draft reports
        - Slight differences are ok
        - Could discuss via conference call
    - Adoption/awareness stats that support Safety WG paper would be useful; however, A&A group would not want its information released in other documents prior to its document being completed
    - Safety and MPC papers should be released together
- Beware of rewriting work that has been done before, e.g., Microsoft paper on appropriate release of vulns – citation in Safety draft
- Public comment timeline:
    - First need to make sure draft reports are not in conflict
    - Coordinate with board of directors at FIRST on MPC
    - January-February public comment period
    - Keep in mind timeframe – 2-3 big cybersecurity papers to be released in December; first half of January would be good as well. Decisions will be made as new administration gets started on how to approach cybersecurity. Papers will be better heard if they come out before a new administration begins.
    - This is focused on industry, not Washington
    - Objective should be to sustain attention on process through transition
    - Comment process can get attention, awareness
    - Could publish document in December that welcomes feedback and is revised later; we will also be getting comments on the drafts that were shared last week
    - Concern that ongoing production may not produce markedly better results (avoid redundancy, rework of concepts, ISO standards already did this)
    - NTIA would be open to getting documents out in the near term and then revisiting at a future point if the group was interested

- When can we come out and say there is no one size fits all but here is some guidance; what do we need?
    - Ensure coordination between two groups with drafts
- FAQ
- Need to define comment period
- A&A WG will share bullet points
- Safety WG draft Wed Nov 23 for comments
- Multi-Party WG draft TBD
- Comments between WGs due in 2 weeks – Nov 21
- Transmittal letter/memo from NTIA would be helpful if possible

- Next meeting: at RSA (Feb 13-17)?
    - Discussion on strategy to drive adoption?
    - Very busy week, schedule challenges
- Launch event should not be at RSA – RSA is not the target audience for this; RSA may also be late
- HIMSS is good audience for awareness and adoption, end users and manufacturers; federal health IT pavilion (PSAs, videos on loop) – opportunity for outreach
-