***This document was compiled in real time from the stakeholder discussion on "key issues" at the September 29 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-process-cybersecurity-vulnerabilities*

Front doors don't work – relationships do work to get things done

Public exposure has tended to lead to results; but also leads to cynicism

Safety concerns (especially with health, transportation, etc.) should be considered

Vendor-side principles

What is a "known-bad"? What are the procedures to address "known bads"?

-known bad – lots of users would be hurt if not fixed

Should society determine how to respond to "known bads"

Compliance standards?

How to reward mitigation?

What about the flip side, where it is cheaper to sue the reporter of the problem.  Cheaper to bury than to address.

Power imbalance – large vendor v. independent researcher

Protection for researchers – lack of process for protection

Why are lawyers involved at all?  Key takeaway for vendors – escalating to lawyers not helpful – keep lawyers out.

Everyone is doing for safety and security reasons – not necessarily adversarial

Chilling effect on researchers – CFAA – criminal and civil

Legally binding covenant for vendors – "we will not take civil action"; civil contract

In free market, would lead to your products being better – more disclosure to you to amend product

Framework for how researchers should engage companies (could serve basis for future legislation)

Cannot just be email address; other components required

Vendor perspective – much distrust between vendors & researchers; vendors might create document, a promise to researchers

Vendor-to-vendor communication/collaboration

Researchers must understand multi-vendor problems may take longer to remedy

Need a “Where We Are At Map”

-when full disclosure?

-when other disclosure more appropriate.

Discussion of external and internal economics

-prices companies are paying for vulnerabilities

-external incentives – what does it cost for companies that have been breached?

-certain incentives are lacking

-this data could be useful for presenting to other SHs

Difference in process from operational perspective depending on software, installed code, hosted code – too much blending; threads are divergent

Operational process about managing disclosures – inherently inefficient – what guidelines for vendors to respond and information shared with researchers so that they have empathy with vendor considerations in response

Vendor-to-vendor (V2V) still major problem – connecting all players difficult

FIRST SIG – open forum; SIG meets twice a month; coordination between vendors on multi-vendor issues difficult; difficult to find the vendors; no directory

Multiple stakeholders – industry, independent researchers – should independent researchers have a dedicated organization; have publicity campaign; get companies to understand what benefits you bring economically, security perspective

Researchers to work together as a group to allow faster results? DoC to coordinate?

Vendors may be unaware of how and who to coordinate with; how to map out vulnerability disclosure – that work is underway. There is a guideline, although many are unaware. Vendors not starting at ground zero, but there is an awareness problem. Much unawareness of resources among all parties.

Determine what already exists, increase awareness, and then determine gaps

Select prior history of disclosure debate needed; bibliography

Other efforts: open security foundation-vendor directory; hacker one directory

Group should highlight prior efforts (seconded)

Researchers should not be expected to identify everyone affected before disclosure; best efforts

Combination of coordinated and full disclosure may be appropriate in certain large scale, coordinated situations

Current issue – software embedded in expensive devices – cars, planes, making it hard to research

Should be rule – no harm to the researcher

If doing research to a service – this could have harm on users – how do you conduct research without causing harm to users

Embedded software – vendors hiding behind IP laws – shouldn't be able to hide, but legitimate IP protection required

3rd party libraries – why are vendors using code developed say in a basement? What is your accountability? If you shipped the code, should you have a process to mitigate any problems in the code?

How to bring the perspective of smaller companies into consideration here?

Is there a different process for designs that don't have public safety implications? How to address economic/security balance for smaller companies with limited resources?

How to ensure multiple scenarios and platform considerations are considered in this process?

Business decisions versus security calls?

Tremendous amount of work that can be done in advance. Vulnerabilities will be found. Cyber Supply Chain Act – if you ship stuff you need to know what you are shipping. Organizations/developers/vendors should have remediation plans so that if a flaw emerges can respond in faster time.

Process should identify pain points that create expensive demands on vendors – can we start funding things that would make this eventual remediation cheaper. What steps can we take in anticipation?

Ability to respond is minimal table stakes. Do we need to institute fire drills? Should we draft disaster discovery scenarios? Go through the paces ahead of time. Improve supporting processes – not just design but other supporting practices.

Value to the process – take the shared experience in the room and help to share that with the newer players. Share the wealth of experience to improve knowledge of practices/principles/approaches.

Zero days – the presumption that there is harm upon public disclosure is false.

What steps should vendors take to be prepared for disclosures; standard processes in place.

Needs to be a middle ground between zero days and letting the vendor sit on it forever. Perhaps middle ground way to expose some details.

Losing trust in the systems that are built is a real risk. Uncertainty is the enemy of trust. There is also uncertainty in the disclosure process.

Uncertainty in civil liability. No class action cases yet, but could be coming. Changing connectivity on things like cars changes the threat model. We must be able to trust systems. Must have a path to fixing larger scale problems as well.

Need more certainty re: how gov't agencies will respond to researchers.

Important to distinguish between who is a bad guy and who is a "good guy researcher." In doing research, they tend to look pretty similar.

Others would caution against trying to make these determinations. Attempts to make determinations between legitimate and non-legitimate research "cause madness." Others see easy distinctions – bad guys will not tell you there is a vulnerability. If they've told you about the vul, they are implicitly "good."

At this point we should be able to say what disclosure looks like when we do it "normally" and we should be able to say "these things are ok". And then if there are requests for adjustments, we at least know what the norms are.

Can we describe a perfect state? And then begin to discuss what goes wrong from there?

Release of exploit code – how do attacks occur following that? Report on this should also look at how attacks occur following patch release.

Can an outsider join FIRST to participate in SIG? Yes. Contact working group.