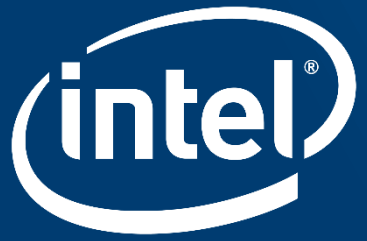
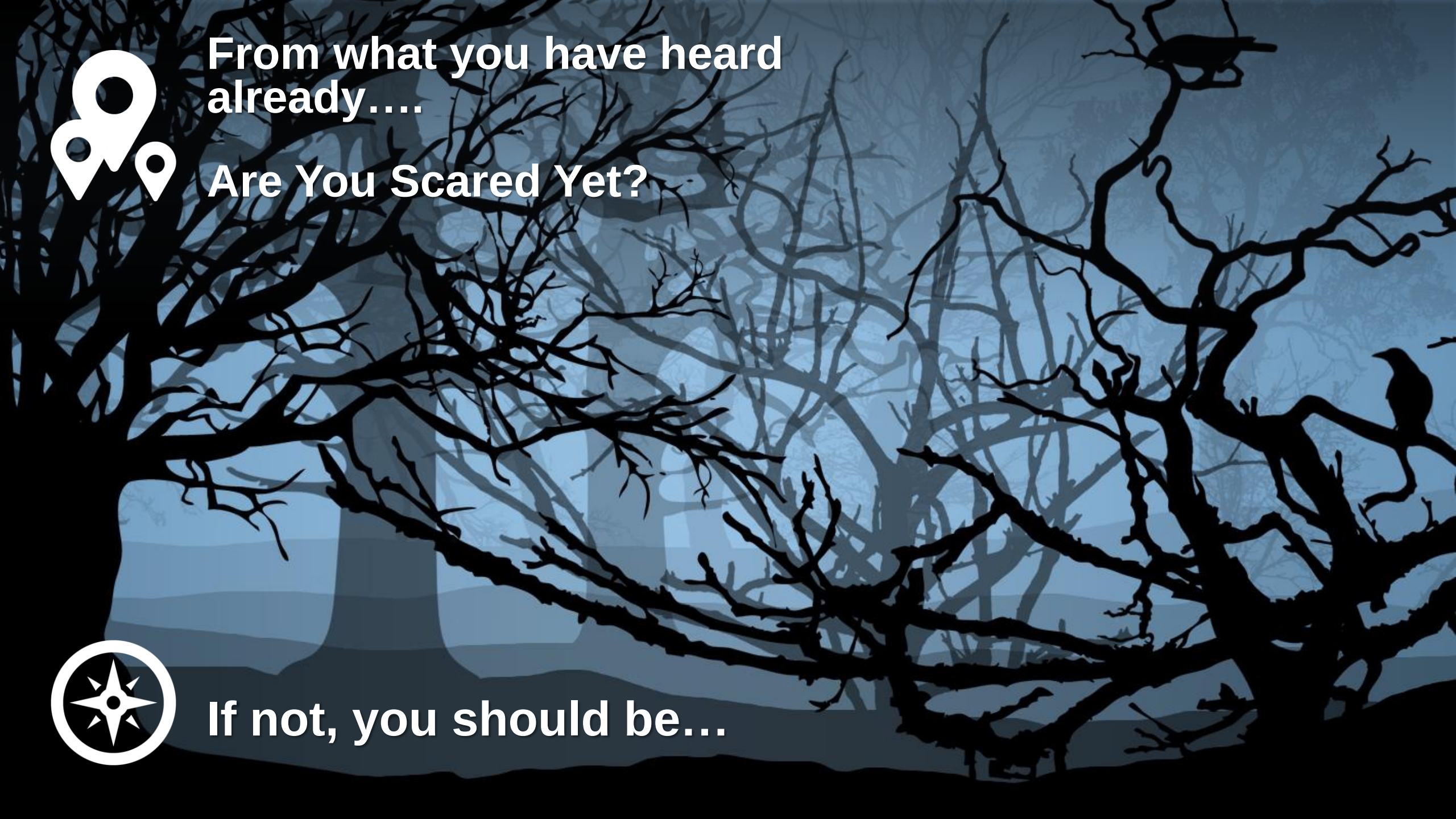


Foundational Cyber Threat Ecosystem Issues

And how USG may be able to help

Kent Landfield, Director Standards and Technology Policy

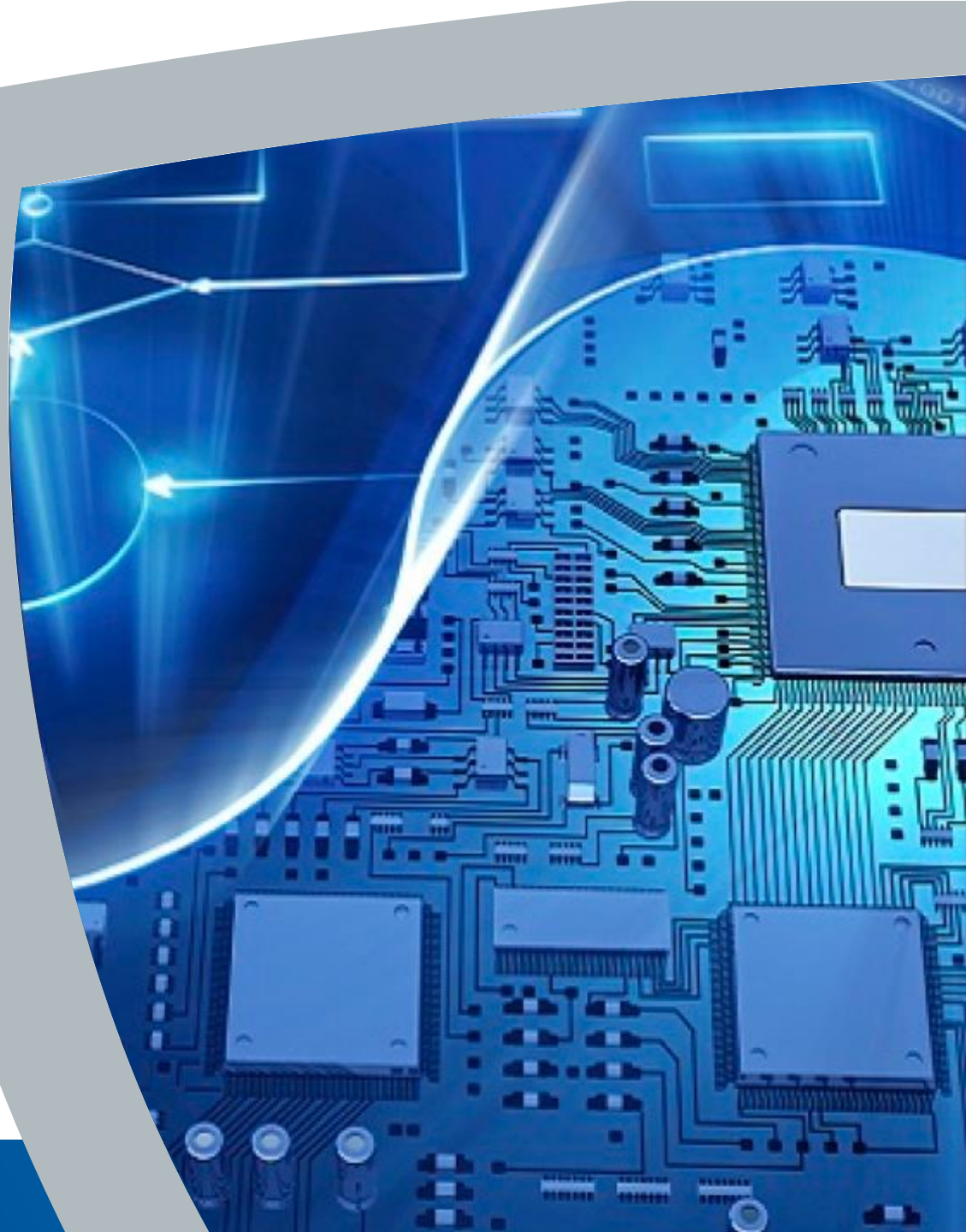

From what you have heard already….
Are You Scared Yet?
If not, you should be…

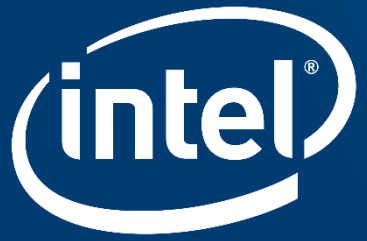
Agenda

- **Vulnerability Disclosure**
- **Vulnerability Identification**
- **Cyber Threat Intelligence Sharing**
- **And one more thing…**

Vulnerability Disclosure

- **No longer limited to computer and legacy software**
- **Expanding into companies that have no idea what a vulnerability disclosure process is**
- FIRST.org Vulnerability Coordination SIG
- NTIA – Multi-stakeholder Process: Cybersecurity Vulnerabilities
- Duplication between the efforts identified and in the December NTIA meeting it was agreed the to merge the creation of the disclosure process work with the FIRST Vulnerability Coordination SIG
- How does the vulnerability disclosure process affect the security of government systems and government policy related thereto?
- **Recommendation:**
  - Support the work FIRST and NTIA are developing





Vulnerability Identification / Reporting

Vendor Vulnerability Identification Usage

Vulnerability Management Technologies

- Detecting vulnerabilities in the deployed environment
- Patching / remediating vulnerabilities
- Reporting security posture status for organizational uses

Vendor security related bulletins and advisories

- Microsoft, Oracle, Cisco, Adobe, Intel Security, etc.
- Compliance

Information Key for security related databases

- Research
- Reporting

Industry Vulnerability Identification Usage

Information Sharing between organizations or departments

- Incident Handling
- Operational security posture tracking
- Security investment success

Tracking method for use in determining the trending and scope of vulnerabilities

- Costing
- Awareness of the problem

Common means to indicate that a single software vulnerability is a single condition

- Unidentified vulnerabilities can appear as multiple problems when reported by multiple vendors

Existing Vulnerability Landscape Problems

Blind, Deaf and Dumb

- CVE has been the foundational means for vulnerability identification
  - English speaking for the most part
  - For the most part…. software vendors have been totally focused on CVE as the sole means for vulnerability identification
- Regional uses for vulnerability identification masks the problem
- National / Regional means for identifying are lacking
  - Some are established and correlated with CVE
  - Some are immature in their process development
  - Some don't exist at all
- Large geographically dispersed software development markets have no real established vulnerability identification programs that are visible to vendors and the regional community they were written for
- Vendors can't assist checking or correlating or protecting against vulnerabilities they do not know about

Current CVE Concerns

- Management of CVE has been under funded for many years
- CVE's are targeting US software/English speaking software only
- CVE has a limited set of sources / products they are tracking and creating CVEs for
- Open source software is not well covered from a vulnerability perspective
- Delays in getting CVEs issued is causing real angst in the researcher community
- The CVEs existing today are very limited compared to the overall software market
- CVE does not do hardware (except a couple joke type entries)
- The increase of new types of hybrid hardware/software sensor / emerging tech is not being addressed by CVE (Think healthcare devices)
- There is a rampant misunderstanding of what CVE is, what it covers and what it provides from a vulnerability management perspective
- *And now legislators have been discussing using it as a measurement for software procurement quality.... (Royce bill is an example)*

Making it better

- Vulnerability identification is critical to the threat landscape and will become more critical as the explosion of new and cheap devices invade our lives, homes and transportation.
- Need to have the CVE program revamped to address the changes to the digital economy
- Means to identify vulnerabilities is critical to our shared existence
- CVE has been overlooked too long and now is the time to shine the light on the issues and plan for the future
- This is a US problem with a global impact

Cyber Threat Information Sharing

- Should Cyber Threat Sharing be the only focus?
- Cyber-Physical is driving us more into more holistic model
- New models for Threat sharing are emerging
  - Cyber Threat Alliance – active CTI
  - ISAO redefinition
- CSA is affecting corporate lawyer perspectives
- EO 13691/ DHS ISAO Guidelines Development
  - All I can say is it is a work in progress….

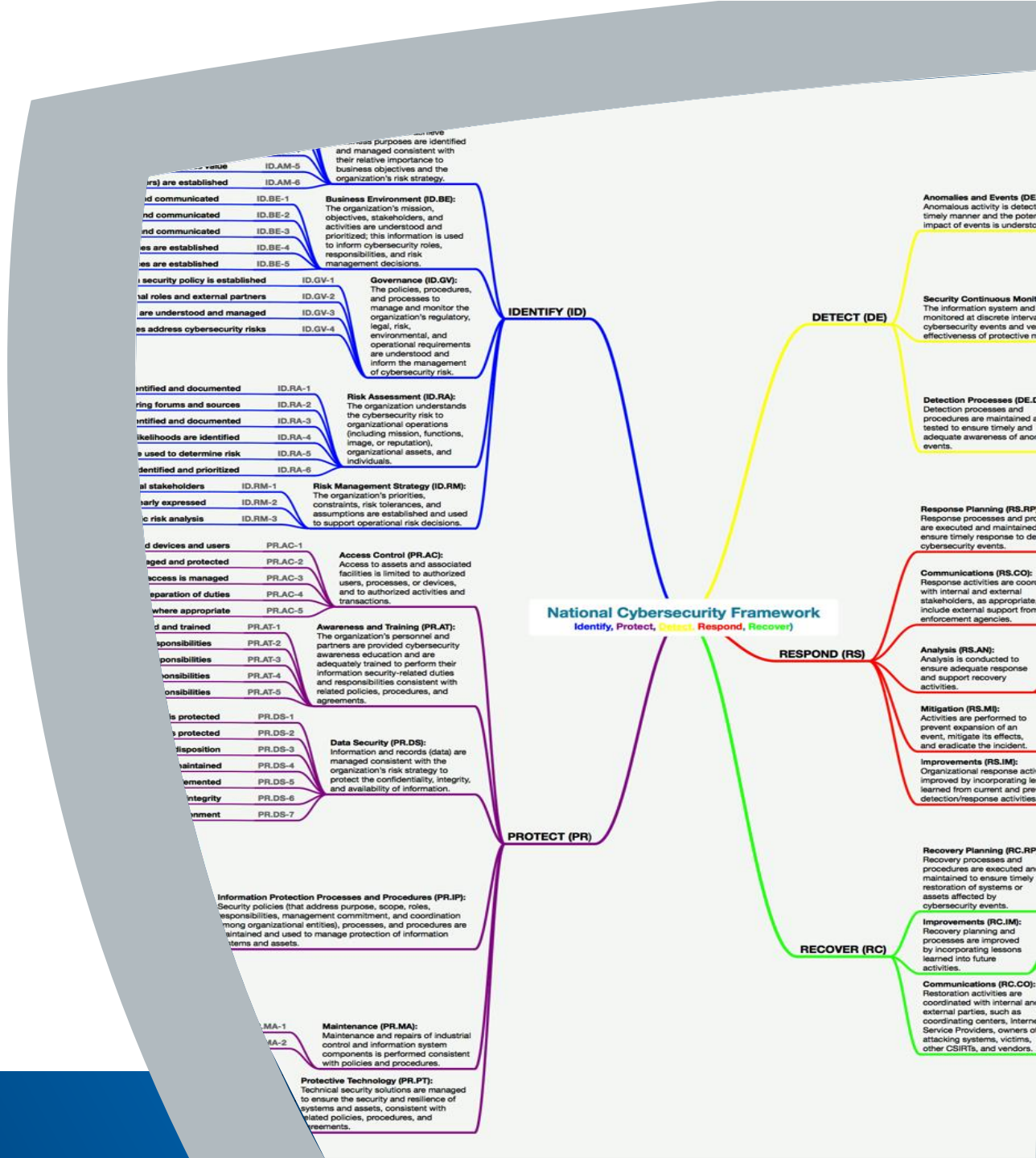
The CTI sharing landscape is evolving...

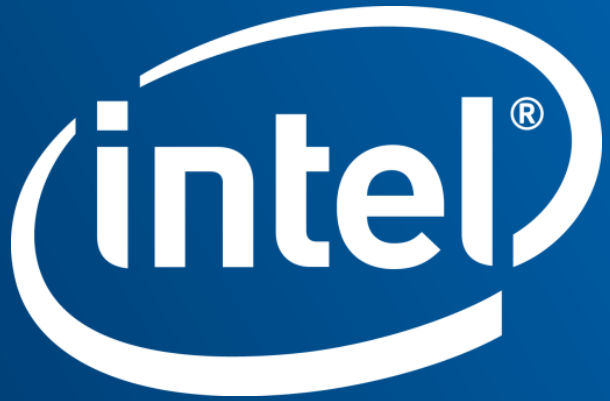
And one more thing…

The Cybersecurity Framework is well received and a powerful tool but it is missing aspects important to the cyber threat landscape.

- Cyber Threat Management
- Cyber Threat Intelligence Sharing
- Tier integration of ecosystem participation

- **Recommendation:**
  - Encourage the inclusion of these components into the next version of the CSF





This presentation is for informational purposes only.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel, the Intel logo, Look Inside., and the Look Inside. logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2015 Intel Corporation. All rights reserved.