U.S. Department of Homeland Security (DHS)

Professionalizing the Field of Cybersecurity Incident Response

30th Annual FIRST Conference, Kuala Lumpur, Malaysia
June 29, 2018

Tom Millar

Homeland Security

TLP:WHITE

Disclaimer & Notification

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

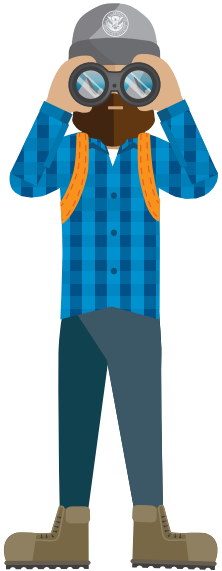
The display of the DHS official seal or other DHS visual identities shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see http://www.us-cert.gov/tlp.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

TLP:WHITE

Who am I?



Member of US-CERT since 2007

- Served as a Network Analyst, Senior Watch Officer, and Chief of Communications
- Led the implementation of Traffic Light Protocol (TLP) across US-CERT's entire product line beginning in 2011
- Supported initial conception and development of the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)

Currently assigned as a Technical Advisor to the Under Secretary of the National Protection and Programs Directorate in DHS

Co-chair of the FIRST Traffic Light Protocol SIG and FIRST Ethics SIG

TLP:WHITE

Professionalization: What it Means

"To make an activity into a job that requires specialized education, training or skill"*

Professions are more than just specialized work, however. Consider:

- Doctors
- Nurses
- Lawyers
- Accountants

All of these fields have another thing in common besides specialized knowledge. They require, and provide, trust and confidence.

*(from http://www.learnersdictionary.com/definition/professionalize)

Building Blocks of a Profession

"A profession relies on **specialized knowledge and skills that require a long period of study;**

The occupational group **has a monopoly on the carrying out of the occupation**;

The assessment of whether the professional work is **carried out in a competent way is done by, and it is accepted that this can only be done by, professional peers**;

A profession provides society with products, services or values that are useful or worthwhile for society, and is **characterized by an ideal of serving society**;

The daily practice of professional work is r**egulated by ethical standards, which are derived from or relate to the society-serving ideal of the profession**."*

*https://plato.stanford.edu/entries/technology/

TLP:WHITE

From Here to Professionalization: Gap Analysis

Current certification and education schemes are “in the middle” - technical, vocational training, tests of overall knowledge, some with limited codes of conduct.

We may need a range of certifications, academic / educational tracks, and associations - similar to nurses and surgeons, or global, management and public accountants, or regional / local bar associations.

Regardless, **we need to acknowledge the society-serving ideal of our career field**, and that must be reflected in our ethics and conduct.

TLP:WHITE

What, Who, How? When AND Where?

- An accreditation system of peers is necessary, and it has to start somewhere.
- A diverse coalition of experienced and respected members of the field is also necessary
  - \+ it will also be necessary for them to agree on things (yes, I know)
- Organizational and funding models have to be sorted out, but should not come before the principles and long-term goals of the field.
- The time is **NOW** - the technical has become political, and our field is lacking a unified voice in matters that affect our work (another thing that professional associations can do).
- “Where” - choosing the forum or venue in which to do this work - is up to us.

Homeland Security