Department of Commerce

Proposed Presentational Abstracts for

NOAA’s Cyber Security Conference

30 April – 4 May 2018

Office of the Chief Information Officer

Office of Cyber Security & IT Risk Management

Rod Turk, Acting Chief Information Officer, Department of Commerce

Ja’Nelle DeVore*, Acting Chief Information Security Officer, Director of National Security Solutions and Services (NS3)

Amy Hintz*, Branch Chief, IT Risk Management Services, Acting Director of Office of Cyber Security and IT Risk Management

Office of Cyber Security and IT Risk Management Team: Marianne Belotti*, Rose Bernaldo, Jeffery Bowmar, Eric Cline*, Abner Desir*, Maria D. Dumas*, Kimberly Ferguson, Cara Huang*, Gordon Keller, Patty McMahon*, Taunya Sills, Nathan Thweatt*, Wendy White-Sellers*[1]

[1] *Individuals listed with an asterisk (*) beside their names are identified as presenters.*

Contents

Cyber Security Industry Innovation

Machine Learning in Cyber Security

Presenter: Ja'Nelle DeVore

According to the National Science and Technology Council, "machines have surpassed humans in the performance of certain specific tasks, such as some aspects of image recognition. Experts forecast that rapid progress in the field of specialized artificial intelligence will continue. Although it is very unlikely that machines will exhibit broadly-applicable intelligence comparable to or exceeding that of humans in the next 20 years, it is to be expected that machines will reach and exceed human performance on more and more tasks." Mike Maraya discusses how cybersecurity professionals could use this emerging technology to make better risk-based decisions.

IT Security Baseline Policy

Introduction to the IT Security Baseline Policy

Presenter: Patty McMahon

DOC's enterprise IT security policy has recently been updated. This session will provide an overview of the changes from the previous 2014 DOC IT Security Program Policy, and provide a look ahead at future planned updates.

Supply Chain Risk Management

Understanding Supply Chain Risks and DOC Requirements

Presenter: Amy Hintz, DOC OCIO

The ability of the Department to identify cybersecurity risks, protect our environment, detect the presence of malicious activity, respond to its presence and recover is greatly enhanced when everyone is focused on cybersecurity. This includes making supply chain risks a consideration in all procurements, in all hardware refreshes and in all software acquisitions and development. The Department's supply chain program is designed to help raise awareness of supply chain risks, how to better identify supply chain risks, understand the effect it can have on our security and what DOC has implemented to meet the challenge.

Continuous Diagnostics and Mitigation

The Present and Future of CDM

Presenter: Cara Huang

Thanks to the hard work of the bureaus, the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program is improving cyber security across the Department by providing near real-time cyber security information. Along with DHS, in this session, we will provide updates on CDM Phase 1 (Managing assets) and 2 (Managing people), and learn what to expect from Phase 3 (Managing events).

Enterprise Cybersecurity Monitoring & Operations

Facing the Challenges of a Continuous Monitoring Program

Presenter: Abner Desir

The challenges of implementing a centralized continuous monitoring program in a federated environment can appear insurmountable. Agency Bureaus and Offices have different culture, IT visions, and risk appetite that cloud the big picture but at the same time present unique opportunities to improve cybersecurity. This presentation provides insight into how DOC integrates people, processes, and technologies to meet its challenges and build a resilient Enterprise Cybersecurity Monitoring and Operations (ECMO) program that is poised to evolve with the cybersecurity risk management landscape.

Enterprise Security Operations Center

Armed and Ready!

Presenter: Nathan Thweatt

Cyber threats are continuing to rise, and therefore, remain a serious economic and national security challenge. The techniques, tactics, and procedures (TTP's) employed by malicious threat actors to breach networks and steal confidential information is rapidly becoming more and more sophisticated. The Department of Commerce (DOC) Enterprise Security Operations Center (ESOC) plays a critical role in the detecting, analyzing, and responding to cyber incidents across the Department. The success of the ESOC relies heavily on the ability of the cyber analyst and incident responder to be "armed and ready" to take on the ever-evolving cyber threat landscape we face today. This presentation will highlight the benefits of having a well-versed cyber workforce that is prepared to address these threats.

Cyber Security Assessment and Management Tool

An Overview of CSAM 4.1

Presenter: Eric Cline

The Department of Justice developed the Cyber Security Asset Management (CSAM) tool, which provides Federal agencies with a web-based secure network capability to assess, document, manage, and report on the status of IT security risk assessments and implementation of Federal and NIST developed IT security control standards and policies. CSAM is also a centralized system for the management of Plan of Action and Milestone to include creating, tracking, and closing, as well as automates system inventory and FISMA reporting capabilities. Join the DOC OCIO and DOJ on a CSAM discussion with a special emphasis on control authoring and inheritance.

Cybersecurity Training Opportunities

Cyber Risk Management Training and You!

Presenter(s): Eric Cline / Maria Dumas / Patty McMahon / Wendy White-Sellers

Please note: the below information of proposed course listings is notional.

In the ever-evolving world of cyber innovation, it is imperative that the government's cyber workforce is prepared to not only respond, but to also take a proactive, risk-based approach in IT security for the workplace. As a result of the role out for new IT Security Baseline Policy, the DOC OCIO will offer a few courses that give insight on bringing policy to action. In collaboration with NOAA's Cybersecurity training program, the DOC OCIO offers the following courses to be launched this year:

- CSAM Overview
- IT Security Baseline Policy
- Risk Management Framework (RMF) Overview
- POA&M Management
- Systems Security Plan

During this session, the DOC OCIO will provide a brief overview of what these courses will cover and will discuss opportunities for training. We will also provide information on other training opportunities that cyber professionals may want to explore.

Resiliency Engineering

Advancing Security by Accepting Failure

Presenter: Marianne Bellotti

When systems grow to a certain level of complexity and scale, avoiding failure becomes impossible. Rather than adding more and more controls to enhance security, the top tech companies embrace failure and focus on Resiliency Engineering. This presentation will cover programs run by Google, Amazon and Netflix and outline ways agencies can incorporate this philosophy into their own software development while still satisfying all their traditional requirements.