

# HIMSS NCA Chapter – January 11, 2018

## Defining a Cyber Moonshot for the Health Industry

### Panelists:

#### **Christopher Wlaschin, Executive Director, Information Security and Chief Information Security Officer (CISO) - U.S. Department of Health and Human Services (HHS)**

Chris Wlaschin oversees cybersecurity for the Department of Health and Human Services, as well as the Office of Information Security (OIS) in the Office of the Chief Information Officer (OCIO), and is the Chief Information Security Officer (CISO). As the Executive Director he is responsible for leading the HHS team in innovation for cybersecurity, as well as building collaboration and sharing best practices across both private and public sectors for information security.

Before joining the HHS team, Chris served as the Senior Director for Information Security and Infrastructure for NRC Health, as well as the CISO for the University of Nebraska system. Prior to that, Chris was the Associate Deputy Assistant Secretary for Security Operations, Information Security for the Department of Veterans Affairs. Chris also served as Chief Information Officer (CIO) for the US Navy's Military Sealift Command.

Chris also served with distinction in the US Navy for over 28 years in a variety of leadership roles.



#### **Emery Csulak, PMP, CISSP, Chief Information Security Officer (CISO)/Senior Official for Privacy, Centers for Medicare & Medicaid Services (CMS)**

Emery Csulak is the Chief Information Security Officer (CISO)/ Senior Official for Privacy for the Centers for Medicare and Medicaid Services (CMS). He leads enterprise and privacy functions at CMS and ensures the Agency complies with secure IT requirements while encouraging innovation.

Recently, as established under the Cybersecurity Act of 2015, he co-chaired the Health Care Industry Cybersecurity Task Force to analyze the challenges the health care sector faces when securing and protecting itself against cybersecurity incidents. Mr. Csulak has over 20 years of experience in information technology, information security and management consulting.

As information technology has grown more complex with the advent of innovative technologies that allow for the rapid collection, storage and distribution of vast amounts of information and data, so too has the importance of safeguarding the privacy of health and other sensitive information collected by CMS. Our Agency is entrusted with the health information of over 100 million Americans, and it our fundamental responsibility as stewards of this information to ensure its confidentiality is protected. Emery leads CMS's efforts to ensure we meet the standards of excellence demanded by that stewardship responsibility, and protect it from bad actors both foreign and domestic.

Prior to CMS, Mr. Csulak was the Deputy CISO for the Department of Homeland Security (DHS) where he developed the DHS Information Security Performance Plan and Scorecard in support of the Federal Information Security Management Act (FISMA). While at DHS, he was a founding member of the Federal Risk and Authorization Management Program (FedRAMP) for Cloud Computing adoption with the federal government. He served as the DHS Technical Representative supporting the Joint Authorization Board (JAB).

Mr. Csulak is a certified Project Management Professional (PMP) and Certified Information Systems Security Professional (CISSP). Mr. Csulak has a M.S. in Software Development Management and a B.S. in Electrical Engineering. Mr. Csulak is a two time Federal 100 Award Winner by Federal Computer Week in 2012 and 2014.



## Defining a Cyber Moonshot for the Health Industry

**Omar Cruz, Project Manager, National Cybersecurity & Communications Integration Center (NCCIC), Threat Analysis Branch, Department of Homeland Security (DHS)**



Mr. Omar Cruz is a Project Manager responsible for leading efforts within the National Cybersecurity & Communications Integration Center (NCCIC) to help improve technology solutions for data analytics that enhances the Computer Network Defense (CND) Mission. Mr. Cruz most recently served as the Branch Chief for Cyber Threat and Information Sharing at US-CERT where he managed a team responsible for researching developments from nation-state Cyber Threat Actors, assessing for changes in their Tactics, Techniques and Procedures (TTPs), and identifying new Indicators of Compromise (IOCs) that could be use for CND Mission. Mr. Cruz contributed to the Information Sharing mission of NCCIC and US-CERT by managing the daily operations supporting the Automated Indicator Sharing (AIS) Program, the Enhanced Cybersecurity Services (ECS) Program, the Cyber Information Sharing & Collaboration Program (CISCP) Team, the Mission Partner Embedded Analyst Program (MPEA) Team, organizing and hosting the monthly classified Joint Agency Cyber Knowledge Exchange (JACKE) cyber threat briefings, managing the US-CERT Mercury Team Portal (US-CERT collaboration platform for Federal CND Community), managing the development of Technical Reports (Indicator Bulletins & Joint Analyst Reports), which were then published to the US Cyber Centers, Federal Departments and Agencies, SLTT, Private Sector and International Cyber partners.

Prior to joining US-CERT in 2013, Mr. Cruz spent over 3 ½ years with FEMA as the Section Chief for Cyber Threat Management, which focused on monitoring, safeguarding, and protecting FEMA's Enterprise Network against foreign and domestic cyber threats. He was responsible for supporting the FEMA CIO and CISO with Subject Matter Expertise (SME) in the areas of IT, IT Security Audit, Cybersecurity policy and Cybersecurity training. He developed the CONOP for the Cyber Threat Management Program at FEMA, successfully transitioned FEMA from a commercial managed service provided to a Federated in-house SOC equipped with malware analysis and computer forensics capability, and provided SME guidance on the handling of all types of cyber security incidents. He supported FEMA's Law Enforcement Unit by personally performing Computer Forensics and Mobile Forensics on all LE related cases. Mr. Cruz has testified in Federal Court as an Expert Witness for Computer Forensics conducted for FEMA.

Mr. Cruz's Federal Government experience also includes time as Deputy Operations Manager for the DHS Security Operations Center (SOC), Operations Manager for the FEMA SOC (managed by DHS SOC), and Team Lead for the Customs and Border Protection (CBP) Computer Security Incident Response Center (CSIRC). In addition, Mr. Cruz served with the United States Marine Corps as a Non-Commissioned Officer (NCO) and completed a 4-year active duty military tour with an Honorable discharge and the rank of Sergeant.

Mr. Cruz received his undergraduate degree in Network and Communications Management from DeVry University in 2005. He is a Certified Ethical Hacker (CEH) since 2007 and Computer Hacking Forensic Investigator (CHFI) since 2013.

### **Moderator:**

**Gus Hunt, Cyber Practice Lead for Accenture Federal, former CTO of the CIA**

Gus Hunt is currently managing director and cyber lead for Accenture Federal Services. He is responsible for developing differentiated approaches to dealing with the cyber threat environment and growing AFS's cyber practice. Previously, Hunt was chief architect and the head of Strategic External Partnerships for Bridgewater Associates, a hedge fund located in Westport, Connecticut. After retiring from federal service, Hunt founded Hunt Technology, LLC, a private consulting practice focused on strategic IT planning, cyber and data-centric security, big data analytics and cloud computing. Hunt serves an advisor for several startups in the cyber-security and big data spaces and serves on the Board of Directors for ePlus, a leading integrator of technology solutions.

### Defining a Cyber Moonshot for the Health Industry

Previously, Hunt served as the chief technology officer for the Central Intelligence Agency, where he was responsible for the information technology strategic direction and future technology investment plan. He was the conceptual and motivating force behind CIA's decision to acquire a copy of both the Amazon cloud and IBM's Watson.

Hunt began his career in 1979 working as an aerospace engineer for Rockwell International and General Research Corporation, designing advanced manned space flight systems and satellite orbital transfer vehicles. He holds a BE and ME in Civil/Structural Engineering from Vanderbilt University in Nashville, Tennessee.

<https://www.accenture.com/us-en/company-gus-hunt>