BUSINESS CASE ANALYSIS FOR A WASHINGTON AIR NATIONAL GUARD CYBER-TO-PHYSICAL SYSTEMS CENTER OF EXCELLENCE

EXECUTIVE SUMMARY

As cyber threats to United States infrastructure and resources become more prevalent, a growing premium is placed on recognizing military-civilian dependencies and enhancing the security and resilience of interconnected critical infrastructure. For the last 11 years, the 262d Network Warfare Squadron (NWS) of the Washington Air National Guard has been on the leading edge of assessing and securing Cyber-To-Physical Systems (CPS) and Industrial Control Systems (ICS). Recognizing 262 NWS' leadership in this area, Air Force Space Command (AFSPC) tasked the 262 NWS to develop the Defensive Counter Cyberspace capabilities necessary to defend and secure ICS and CPS systems across the Air Force enterprise. This was in accord with the July 2016 "Annual Prioritized AFSPC Air Reserve Component (ARC) Initiatives" priority identified by the Commander, Air Force Space Command, General John E. Hyten. In response to this tasking the 262d has built and is delivering capabilities, component recommendations and operator training for integration into the US Air Force Cyberspace Vulnerability Assessment/Hunt (CVA/H) Weapon System. Further, the Governor of Washington appointed the 262d to partner with the Washington Army National Guard and Washington State Guard to perform an Industrial Control System defense assessment for State Public Utility organizations. This extensive background and experience makes the Washington Air National Guard the ideal DoD candidate to stand up a CPS Center of Excellence to enhance the cyber resiliency of our military critical infrastructure by training cyber forces within DoD as well as outside agencies. This business case analysis explores this Center of Excellence concept by explaining its purpose, discussing potential course offerings, and outlining required resources.

BACKGROUND

"It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof." PPD21 Feb 12, 2013

President Obama formulated PPD21 in 2013 in an effort to define and highlight our nation's dependency on critical infrastructure and the cyber-to-physical systems that this infrastructure relies upon. Since that time incidents such as the Ukraine power grid attacks in 2015 and 2016 have shown how these types of attacks have grown in sophistication and have become a viable instrument of national power for governments worldwide. Former Secretary of Defense Leon Panetta was prescient in his October 2012 warning of the potential for "a cyber-Pearl Harbor" when he noted that the United States was, "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government". While this 'cyber Pearl Harbor' has not yet occurred on US soil, potential and vulnerability make such an attack extremely likely in the future.

Due to the interconnected nature of critical infrastructure, the military is similarly vulnerable to potential cyber-attacks. In their February 2016 letter to former Secretary of Defense Ash Carter, Admirals Gortney and Harris, Commanders of U.S. Northern and Pacific Commands respectively, voiced their concerns by requesting "assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed - cybersecurity of DOD critical infrastructure Industrial Control Systems." Specifically, these admirals pointed out "a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure."

In spite of this emphasis, our country continues to struggle to get the right people with the right skills on the front-lines to counter this threat. Today, the US Air Force (USAF) has only one Air National Guard (ANG) unit tasked specifically to counter cyber threats to Industrial Control and Cyber-to-Physical Systems. Air Force Space Command envisions all USAF Cyber Protection Teams eventually having the capability to evaluate Air Force Industrial Control Systems using the capabilities of the CVA/Hunt Weapon System coupled with training content developed by the 262 NWS. In terms of civilian cybersecurity preparedness, the 2016 DHS National Cyber Security Resilience review found that most state and local governments are below the recommended threshold prescribed by the NIST Cybersecurity Framework. More must be done to identify, train and employ expanded military and civilian cyber capabilities.

CPS CENTER OF EXCELLENCE

The Washington Air National Guard's 262 NWS is based at Joint Base Lewis-McChord, WA. It is comprised of 101 Citizen Airmen, 30 of which dedicated to three CPS Defense Teams.

Since 2001, the 262 NWS has been the go-to cyberspace operations organization for several high profile vulnerability and mission assurance assessments for major combat weapons systems to include a presidentially directed Cyber-to-Physical study of the Minuteman III Weapon System and the B-52H avionics data bus system. Additionally, the 262 NWS has led studies to validate ICS safeguards for Federal, State and other government agencies around the world to include the first ICS assessment on the CAOC at Al Udeid AB. Locally, under the authority of the Governor of Washington State, the 262d performed an ICS assessment on the water and power utilities of Snohomish Public Utility District (SnoPUD). Currently the 262d is tasked to evaluate life sustaining ICS systems at McMurdo Station, Antarctica and critical ICS systems for the Pentagon. Collectively, these missions have fostered a level of CPS defense expertise that is unique within DoD. It is this depth of experience as well as the civilian talent of its traditional Airmen that will form the core of the new Center of Excellence.

Finally, as part of its mission to develop a CPS defensive capability for the US Air Force, the 262d staff has designed and written a basic CPS security course and Concept of Employment for performing CPS security missions using the newly enhanced CVA/H Weapon system. While designed to serve as a CPS Specialized Mission Qualification (SMQ) within the Cyberspace Protection Teams (CPT) capabilities, these efforts by the 262d provide an outstanding foundation for expanded course offerings and present an opportunity to leverage existing efforts to get the Center of Excellence concept operating in minimal time.

PARTNERSHIPS

While benefiting from close proximity to numerous technology-centric companies that employ many of our Drill Status Guardsmen, such as Microsoft, Amazon and Boeing, the Washington Air National Guard has also benefitted from the foresight and vision of its state leadership. In January of 2016, Washington's Governor Jay Inslee announced, "an innovative partnership with the U.S. Department of Homeland Security to strengthen the protection of critical infrastructure and government services," to enable, "new ways for state government to defend against increasingly sophisticated and targeted cyber threats." While covering many aspects of his "community cyber" approach, a key enabler for this new policy was the outreach and partnerships that the Washington National Guard had already established with key governmental entities within the State.

One of the earliest of these relationships was a partnership with Idaho National Labs, one of our nation's foremost authorities on running and securing critical infrastructure supporting utility delivery systems. This partnership was one of the first of its kind between a National Guard (DoD) entity and a National Lab (DoE) entity in the area of cyber security. The result of this partnership was advanced training for Washington Air National Guard members to secure ICS and, later, developed into a methodology to assess Air Force specific systems.

While the skill sets of the WA ANG matured, so did its partnerships. Over time, these partnerships extended to a number of DoD and non-DoD entities:

- Air Force Civil Engineering Center (AFCEC): Key partner in exploring partnership opportunities between the US Air Force Civil Engineering and critical infrastructure security entities
- Pacific Northwest National Labs (PNNL): Supplied hardware and systems expertise for ICS modifications to the CVA/Hunt weapons system
- United States Cyber Command (USCC): Worked to establish/test alternative structures for a CPS defensive team; resulted directly in the ten person CPS UTC model
- Snohomish County Public Utility District (SnoPUD): Partnered to perform one of the first cyber security assessments of a State-run utility company

As Governor Inslee stated, cyber security is a community endeavor. The breadth of the relationships that the WA ANG has developed over time demonstrates its strength and leadership position within the critical infrastructure

community and highlights the diversity of skillsets and perspectives that it can bring to a future CPS Center of Excellence.

RESOURCES

As a part of the proposed Center of Excellence, the schoolhouse will consist of a squadron of 50 personnel (32 Full-time and 18 Drill Status) comprised of administrative staff and two cadre flights focused on a variety of CPS/ICS topics at varied levels. The facility will support both unclassified and classified training and consist of three classrooms, each designed for a maximum of 30 students and outfitted to deliver expert level instruction in hands-on laboratory environments.

SCHOOLHOUSE CAPABILITIES

The schoolhouse will offer three different courses that can be expanded over time, offering a total of 17 classes annually. The first course would be a USAF CPS course specific to CVA/H; second, a non-service specific CPS course tailored to government, industry and academic partners; and third,, an advanced CPS course. The first course would be our two week CPS/ICS SMQ course designed specifically for US Air Force CVA/H Weapon System operators giving them an understanding of how to provide Defensive Cyberspace Operations using the CVA/H Weapon System. Students successfully completing the CPS/ICS SMQ course would be awarded the US Air Force CPS/ICS Specialized Mission Qualification (SMQ) on the CVA/H Weapon System and would be eligible to take the advanced course. The second course is a "Joint CPS" course designed for non-CVA/H Weapon System services and external industry/academic organizations providing an understanding of processes, concepts and procedures of non-platform specific Defensive Cyberspace Operations and making them eligible for the advanced course. Finally, the advanced CPS course is designed to provide advanced techniques and procedures for operators specifically focused on Industrial Control Systems advanced topics and deeper dive discovery capabilities. The schoolhouse facility will be able to support 30 students per course resulting in a maximum throughput of 370 highly trained operators per year.
Once resources are received, the schoolhouse will be capable of offering the CPS/ICS SMQ course within approximately six months. This will provide initial throughput of 100 students in its first full year of operation. This startup period will allow the Schoolhouse to establish itself while hiring key members to continue developing a more robust curriculum for the Joint CPS and advanced courses. The schoolhouse will phase in the Joint CPS course and the advanced course at the beginning and end of the second year respectively.

The Washington Air National Guard is nationally recognized as having the preponderance of forces, capabilities, and specialized skills to establish a Cyber to Physical Systems Center of Excellence schoolhouse. We stand ready to answer the national call to strengthen the security and resilience of the nation's critical infrastructure against cyber threats.