Nuggets of Wisdom: How to have a Successful Career in Critical Infrastructure Protection.

As I began to look back and think about some key learnings for success while working in the Critical Infrastructure Protection field, I was reminded of the vision statement from the National Infrastructure Protection Plan (NIPP) NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. The vision states that: **A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.**

This vision drives the basic approach to strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community. So, I have compiled 5 key learnings that should facilitate success as a Critical Infrastructure Protection Professional (CIPP):

Key Learning # 1: Remain Secure and Resilient. As a CIPP, success comes when there is a deep personal commitment towards continuously training and educating oneself within this arena. Not to mention, maintaining the high-level skillset it takes for sustaining a world class resilient CIP program. For me personally, it would have been extremely easy to become complacent and simply accept the status quo as it related to having multiple professional certifications, areas of responsibility, job titles, etc. However, my work ethics would not allow me to sit dormant and not explore unforeseen developing horizons within the CIPP field.

A passion for constant learning towards advancements in security, resiliency, and critical infrastructure components took place through attendance to conferences, symposiums and actively participating in bona-fide associations or governmental agencies. One such association that helped is the American Society of Industrial Security (ASIS). ASIS is a long-standing global community of security practitioners, each of whom has a role in the protection of assets-people, property, and/or information. This body of professionals have a myriad of career experiences that could provide a CIPP with techniques and methodologies for shoring up a sound program.

Another resource, Critical Security and Infrastructure Security (CISA), a government agency is one that provides guidance to support state, local, and industry partners in identifying the critical infrastructure sectors and the essential workers needed to maintain the services and functions we depend on daily. CISA's Resilience Services conduct assessments, analysis, and support planning: lead efforts to enhance the understanding of, and drive collective action on, infrastructure security and resilience challenges – by, with, and through integrated planning and assessment capabilities to enhance program resilience.

A significant tool not to overlook in which to further aid in the building and maintaining of a successful program is identifying key business partnerships and the ability to sustain them. This can be done by attending and participating in conferences, joining associations that can add true value to your program and setting up appointments with key sector players in order to align program vision. By doing so, a CIPP can utilize assets and/or resources, such as personnel that may very well be limited within your own organization.

To remain secure and resilient an organization's leadership encourages the CIPP to pursue knowledge base by attending relevant conferences. This requires leadership to fund things like travel, training, and potential opportunities to network with like people.

Key Learning # 2: Minimize Vulnerabilities. Performing effective risk assessments is the basis of a successful Critical Infrastructure Protection program. Risk assessments are crucial in identifying threats, assess and minimize vulnerabilities and evaluate the impact on assets, infrastructures or systems considering the probability of the occurrence of identified threats. This is a critical factor that differentiates a risk assessment from a typical impact assessment methodology. In general, the approach that is used is rather common, consisting of some main elements: Identification and classification of threats, identification of vulnerabilities, and evaluation of impact. This is a well-known and established approach for evaluating risk and it is the backbone of almost all risk assessment methodologies that I've come to use.

A good foundational resource is The Homeland Security Presidential Directive (HSPD-7) established U.S. policy for enhancing critical infrastructure protection by establishing a framework for the Department's partners to identify, prioritize, and protect the critical infrastructure in their communities from terrorist attacks. While utilizing the directive I found it identified 16 critical infrastructure sectors and, for each sector, designated a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programs and activities.

The Department of Homeland Security identified gaps in existing critical infrastructure sectors and established new sectors to fill these gaps. For each Sector-Specific Agency a sector-specific plan was developed for the implementation of the National Infrastructure Protection program (NIPP) in each sector. However, I found that while working in private industry in US CIP there is a tendency to focus more on resilience issues.

Furthermore, the National Infrastructure Protection program (NIPP) is the implementation framework of the US CIP. It provides the guidelines for the implementation and minimizing vulnerabilities of the CIP program. Among others it integrates the efforts for critical infrastructure protection measures in the various sectors, it defines the roles and responsibilities of the several actors at state and federal level and sets the framework for a risk management framework for critical infrastructures.

In my opinion, any successful program would warrant a strategic plan that included the performance of a risk assessment tool for the verification and validation of potential vulnerabilities.

Key Learning # 3: Consequences Minimized. There is an age-old adage that says, "sometimes even the best plans of man may go awry". This may be the case when considering this 3rd key learning I've listed. But, it is one that I have learned that by not paying close enough attention to could spell disaster.

I've learned one of the first objectives in minimizing consequences is to identify and assure the protection of your business assets, and systems that CIPP deem most 'critical' in terms of national-level public health and safety, governance, economic and national security, and public self-assurance. Design, development, and implementation of a comprehensive, prioritized assessment of one's facilities, systems, and functions are key to minimizing program exposure. Not to mention, monitoring the preparedness across infrastructure sectors. However, based upon my past historical performance,

progress has been slow by CIPPs towards a unified approach to critical infrastructure protection even though there are hundreds of tools and methods currently exist for evaluating criticality in infrastructure. Identification and prioritization of the most critical components of a critical infrastructure remains a challenging intellectual problem. This has left the field of critical infrastructure protection without a widely accepted standard approach to vulnerability and risk assessment.

I mention all this to simply let you know that a successful CIP program should not loose insight of any type of consequence that may directly or indirectly breach that program. Being vigilant by auditing and maintaining ones CIP has proven for me beneficial on numerous occasions. Internal audits that my team or an external team found gaps within my organization's policies, procedures, work instructions revealed potential consequences that could have caused major business interruptions at the field operations level causing loss of productivity, revenue and even reputation.

Key Learning # 4: Threats Identified and Disrupted. Within the content of any successful CIP, I have noticed it essential to have any and all threats identified and if possible, eliminated.

For the sake of this paper, I have identified three classes of threats to critical infrastructures: (1). Natural - earthquakes, tsunamis, volcanic eruptions, extreme weather (hurricanes, floods, draught) and fires. (2). Human-Caused - terrorism, rioting, product tampering, explosions and bombing, theft, financial crimes, economic espionage to name a few. (3). Accidental or Technical - infrastructure and hazardous material failures and incidents, power-grid losses, water-treatment facilities failures, water-mains ruptures, safety-systems failures, and a host of other disasters.

Vulnerabilities are characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) because of having been subjected to a certain level of threat or hazard.

I find it long waiting for private industry to meet and exceed critical infrastructure protection standards. Corporate America must step up and meet CIP compliance. Whether it is the physical protection of facilities from vandalism, terrorist acts, and other security breaches, or the protection of IT software and hardware assets from increasingly cyber criminals, it is essential for companies to meet these challenges by updating their CIP policies and procedures annually The decision to not do so can be disastrous, not only for them, but for their longtime client base partnerships. Disaster preparedness or emergency management models and training exercises for the CI program could potentially assist in aiding business interruptions in sectors like, transportation, healthcare, and energy.

Key Learning # 5: Response and Recovery Accelerated. Accelerated assessment of damages to Critical Infrastructure (such as chemical complexes, healthcare facilities, roadways and bridges and other transportation components, energy, food, agriculture, telecommunication, etc.) is corner stone to the post-disaster planning and recovery mitigation efforts. Such planning efforts include creation of temporary shelters, identification of evacuation zones, and optimal placement of first responders, among other human resources.

A coordinated approach is needed that includes multitude of activities: a) Top-down or high-level damage estimation from remote sensing data, b) human in loop validation and verification of CIs that fall in the path of disaster from the previous step, c) Bottoms-up or higher-order feature extraction from spatially-explicit ground-level imagery (also serves as a second line of evidence), and d) information

extraction along with information quality assurance from crowd-sourced data (social media, news, blogs, etc.). Besides, data-intensive computing infrastructure are essential for creating a comprehensive picture of the immediate event aftermath situation and delivering it within 24 hours of post-disaster (called the "Acute Phase") by the U.S. CDC guideline, for maximal effectiveness.

When activated by the Federal Disaster Recovery Coordinator, the primary and supporting departments and agencies deploy in support of the Infrastructure Systems Recovery Support Functions (RSF) mission.

- Supports the recovery of infrastructure systems, dependent on the nature and scope of the disaster, and the specific authorities and programs within the jurisdiction of participating departments and agencies. Participates in the national-level coordination of damage and community needs assessments as appropriate to ensure infrastructure considerations integrate into the post-disaster public and private sector community planning process.
- Deploys Recovery Support Function resources, as required by the specific disaster situation and consistent with the specific authorities and programs of the participating departments and agencies, to the field to assist the affected community in developing an Infrastructure Systems Recovery action plan that: Avoids the redundant, counterproductive, or unauthorized use of limited capital resources necessary for infrastructure/recovery.
- Helps resolve conflicts, including those across jurisdictional lines, resulting from the competition for key resources essential to infrastructure systems recovery.
- Set a firm schedule and sequenced time structure for future infrastructure recovery projects.
- Works with Recovery Support Function partners to leverage available financial and technical assistance, both from governmental and nongovernmental sources, in the execution of the corporation's Infrastructure Systems Recovery action plan. Federal Emergency Management Agency promotes rebuilding infrastructure in a manner which will reduce vulnerability to future disasters impacts.
- Maintains robust and accessible communications throughout the recovery process between the Federal Government and all other partners to ensure ongoing dialogue and information sharing.
- The Infrastructure Systems RSF provides the coordinating structures, framework, and guidance to ensure: Resilience, sustainability and mitigation are incorporated as part of the design for infrastructure systems and as part of the community's capital planning process. Infrastructure systems are fully recovered in a timely and efficient manner to minimize the impact of service disruptions.

The private sector critical infrastructure has the incentive and the means to support a unified community and national recovery effort. The capacity of all infrastructure systems is adequately matched to the organization's current and projected demand on its built and virtual environment.

Well, this comes down to the conclusion of what I think would make a successful CIPP. After 40 years of developing and implementing this type program, not to mention programs within the Health, Safety and Environment discipline at a major oil and gas drilling contractor and an electric utility company there's nothing more satisfying than sharing work-life experiences to all generations. The five (5) aforementioned key learnings I shared should offer organizations some "tried and tested" measures that I think would make a successful CIPP.