"Today, end users bear too great a burden for mitigating cyber risks. Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have significant impact on our national cybersecurity."

- National Cybersecurity Strategy, March 2023

# Resilient Advising Solutions™ Plan and Assess Seminar

*Implementing the DHS State and Local Government Cybersecurity Program*[1]

**Cyber Intelligent Partners** will provide "human centered approach" advising and consulting services for cyber & digital transformation, including information and communication technologies (ICT). Primary focus on risk management and vulnerability assessment for public and private State, city, county, and tribal sector urban and rural entities – emphasizing supply chain & critical infrastructure cyber resiliency planning, K-12 cyber hygiene, and career and technical education (CTE) needs.

**Why?**

- The global digital transformation[2] market size is expected to grow at an annual growth rate of 21.1%, to reach $1.5 billion by 2027 from $594 billion in 2022. The extent of digital transformation had expanded due to shifting consumer preferences and the quick rapid growth of ICT (e.g.), mobile devices and applications or Internet of Things (IoT). The use of cloud services has also expanded, requiring more cybersecurity standards from service providers offering solutions to state and local governments.

- 60% of small-to-medium-sized businesses around the world experienced a cyber-attack in 2020, and 45% of the companies were ineffective at mitigating the attacks. There were 50% more attack attempts per week on corporate networks globally in calendar year 2021 compared with 2020. Education and research were the biggest adversary cyber targets next to government & military, and communications.

It is near impossible to completely protect your business from cyber-attacks, and that is why the **emphasis needs to shift from cybersecurity to cyber resilience**.

**How?** Seminar agenda will incorporate Four-Phase advising:

| | |
|---|---|
| ➢ Gain "State of" cyber integrated with guest speaker to discuss latest updates/trends/threats at strategic and operational cyber levels.<br>➢ Discussion on risk management plan and vulnerability assessment.<br>➢ Review Cyber Threat Intelligence (CTI) capabilities across a traditional intelligence lifecycle to include information sharing/fusion and operations integration. This will incorporate use of tabletop exercise activities and cyber readiness rehearsal.<br>➢ Discuss gaps in solutions space forum. | - **People.** Workforce development and training needs.<br>- **Process.** Governance such as information sharing needs across Fed, state, local and private sector Security Operations Center (SOC) networks.<br>- **Technology.** Need for open-source tools, predictive analysis, data automation, and common operating picture (COP) dashboard or integrated cloud architecture/computing. The COP dashboard could also provide continuous monitoring for ongoing evaluation, grading, and security rating benchmarks. |

[1] www.cisa.gov/state-and-local-cybersecurity-grant-program

[2] Digital Transformation technology components include Cloud Computing, Big Data & Analytics, Mobility & Social Media Management, Cybersecurity, Artificial Intelligence/Machine Learning

[3] Cybersecurity and Infrastructure Security Agency (CISA) provides CISA Tabletop Exercise Packages (CTEPs) as a comprehensive resource designed to assist stakeholders in conducting their own exercises. CTEPs include pre-developed scenarios and module questions to discuss information sharing, response, and recovery elements. Partners can use CTEPs to initiate discussions within their organizations to assess their preparedness for a variety of threats and incidents.

1544 Spring Hill Road, Suite 5115 | McLean, VA 22103

For more information, contact Jeff Hoffmann: jeff@cipsolutions.org or Tel: (703) 424-0233 *www.cipsolutions.tech*

**Deliverables?**

- New strategy or governance document development such as cyber resiliency, threat intelligence program build, or third-party risk management plan, especially for critical infrastructure sectors with large supply chain and high quantity of "outside" vendors
- Facilitation for replacement of legacy tools, systems (networks), applications or introduction of new technologies like CTI analysis, reporting, and information sharing capabilities.
- Workforce development strategies, career path plans, and training platforms, starting with K-12 and CTE.

**Proof of concept:** In addition to the Cyber Intelligence Workshop Forum hosted in 2018, CIP staff and SME experts have over 20 years of experience in the cyber advising discipline. Most recently, the President and CEO (as the Regional Cyber Lead (Europe) for the Defense Security Cooperation Agency, Institute for Security Governance) managed logistics, $250K in resourcing with a team of experts to orchestrate over five Institutional Capacity Building (ICB) - Cyber & Digitization engagements in Romania, Kosovo, Hungary, and the Czech Republic. The teams advised cyber command elements, Presidential staff/council members, interagency, and Ministry of Defense groups on cyber strategy, policy, governance, and law, workforce development, critical infrastructure, crisis planning, SOC infrastructure, and provided incident response training. *Click on image for more details from the 2018 Forum.*

Photo from Cyber Intelligence Workshop Forum hosted in 2018 that included panel topics on cyber strategy, overview of cyber assessment tools, fireside chat on cyber challenges and a cyber threat intelligence analysis war game simulation. The Forum was led by former President and CEO, Michelle Watson, along with special guests like Peter Singer, strategist and fellow at New America and former White House officials on the National Security Council.

Full summary of "Past Work Performance" can be reviewed at:
https://cipsolutions.tech/past-work-performance

**Costs for One Seminar (1.5 weeks):** $158,500

| | |
|---|---|
| Labor (SME expertise): 150 per hour x 5 experts x 64 business hours | 48,000 |
| Guest Speaker Fee: $5,000 | 5,000 |
| Per diem (lodging and meals) - $215 per day in Phoenix (12 days) | 12,900 |
| Transportation (x 6 including guest speaker) est. 650 (roundtrip) | 3,900 |
| Bundling packages (e.g.) Mandiant CTI suite and tabletop exercise requirements ** Includes 2 of 5 SMEs (under labor costs) | 11,480 |
| Admin (Misc.) like printing, marketing material, handouts | 1,500 |
| CIP Operations (e.g.), agenda, material and SME development and prep | 35,000 |
| **TOTAL** | **$117,780** |

**State and Local Security Challenges**

The challenges that cybersecurity professionals face at the state and local level are complex, perhaps even more so than in the national environment. With a broad range of services offered at the town, city, county, and state level, agencies are forced to spread their resources thin in order to secure this infrastructure. Here are five of the most important challenges these state and local agencies face.

- **Sensitive and Valuable Data:** Schools, libraries, police and fire departments, motor vehicle departments, public transportation, roads, and water and sewage systems are all managed by state and local entities. In addition to providing critical services, many of these infrastructures also collect and store citizens' data, making them prime targets for cybercriminal exploitation.
- **Personnel Constraints:** Both the cybersecurity skills gap and the nationwide high-tech workforce shortage have impacted state and, even more so, local governments severely. Attracting and retaining adequately-sized and skilled IT workforces is difficult, especially when competing against the private-sector marketplace for talent.
- **Budgetary Constraints:** State and local governments have always struggled with budgeting, and in times of economic crisis – such as the COVID-19 pandemic – these local jurisdictions have even more challenges to overcome. Cybersecurity is expensive to implement and maintain, and often gets put in the category of a "nice to have but non-essential" budget bucket.
- **Footprint Expansion:** In the face of digital transformation, agencies are being confronted with more software licenses, devices, and services than ever before. Considering the rapid growth in the adoption of IoT and cloud services, it is clear that digital footprints of even small municipalities are becoming more complex to manage. Compound this with the vast number of products installed from different vendors, and it is clear why state and local agencies often struggle to gain full visibility into threat activity, monitor their networks, and secure their connected environments.
- **Compliance:** Less visibility and control over expanding networks means that agency IT teams also often find themselves dealing with compliance-related issues. A large number of employees in a typical state and local ecosystem, combined with the fact that most data breaches happen as a result of human error, only amplifies this challenge.

*Source:* Government Technology article, Richberg, Jim (Fortinet Field CISO and past National Intelligence Manager for Cyber (ODNI), "Today's Cybersecurity Checklist Priorities (Contributed)," May 8, 2020 -- **States and localities face multiple challenges when it comes to data protection. Having the right tools and services in place can make a crucial difference in today's tough cybersecurity environment.**