Federal Facilities Council
Cyber Resilience of Building Control Systems Workshop

Condortech Services Inc. (CTS) recently collaborated with industry peers at the Building Control Systems Cyber Resilience Workshop. The workshop was developed and presented by the Federal Facilities Council through the National Academies of Sciences, Engineering & Medicine, with annual funding coming from multiple sponsoring federal agencies, including the Department of Defense and others. Hosted at the Department of Commerce in the heart of the nation's capital, the event was conceived as a 3-day event for discussing and heightening awareness of measures needed to better protect the intelligent systems that run our nation's federal facilities. Noted was the direct correlation between Physical Security and Cyber Security and the risk inherent from international terrorism and rogue threats.

Among the various presenters who shared industry initiatives to address the need to better secure Federal facilities were a variety of representatives, including Building Controls specialists and government policy makers. The conference was conceived in such a format to cover a broad spectrum of perspectives, all conveying, or rather, promoting awareness of the cyber-risk issue. Steve Stockman, a former congressman, whose cause-célèbre during his tenure was to promote the understanding of vulnerabilities in critical systems of government infrastructure, opened the event as a keynote speaker. Congressman Stockman explained very simply that as the nation is confronting these threats, the best plan is to be prepared – you want people to not know who you are or what you are doing.

John Conger, Asst. of Secretary of Defense for Energy, Installations & Environment, also spoke at the event, explaining that cyber-risk is a problem that we have been creating over many years. Mr. Conger highlighted some of the main issues encountered in this arena. The field of cyber-protection is getting money, but the domain of facilities & building controls as a subset is being delayed. And in preparation, there are not always dual-skill set workers, and the inventory we are supposed to protect can be hard to track. Mr. Conger rhetorically asked, "What are we supposed to do?" Specifically, we have to get every department, every employee thinking about these issues. Cyber experts need to take appropriate documentation and make it easy enough for people to read as a manual and implement needed cyber-protection strategies.

Several grouping of speakers were paired with one another to present different thematic sections throughout the multi-day event. Some of the topics covered included Governance & Policy; Building Control System Vulnerabilities; Federal Cyber-security Acquisition/Budgeting; and Government Tools for Discovery & Assessment.

Speaking on Control System Vulnerabilities, ICS-CERT representative Marty Edwards explained that Industrial Control System infiltrations have been reported to ICS-CERT for quite some time, whereas the agency has been geared toward assessment in the private sector. The need has always been apparent because control systems can affect the economics of a company. This is the forecast that must be embraced by the Federal Government in terms of the same system infrastructure… it is not a matter of if, but when. The federal sector is not paying enough attention yet. Mr. Edwards reiterated that the industry has not yet encountered "the BIG one," namely a huge OT system infiltration, but this begs the question: Are we doing a good enough job looking? Who is doing IP scans of smart light bulbs? Criminals will find out the method and start to implement. The Federal Government has to be ready.

GSA representative Jeff Koses, Senior Procurement official, explained how some practices are already in place, speaking pointedly about risks to Access Control. The Office of Management and Budget (OMB) has steered

efforts to create rules concerning cyber security. This process is thorough, yet long and entails an intense method of reporting information, assessment and continuous monitoring. Achieving the right balance to monitor costs is key and more information is needed by GSA to put these rules in place. Mr. Koses emphasized the need to make such a process easier, and brought forth the suggestions of updating GSA schedules to be inclusive of such changes and to streamline protocol for PACS projects encompassing cyber procedures.

Panel contributors also involved industry representatives from the actual field, including Condortech's own Jorge Lozano, who shared insight from CTS' experience across multiple federal agencies integrating various ESS systems into contiguous infrastructures. Mr. Lozano explained the real scope of the threat, understanding that basic IT understanding must be incorporated into the design of Security systems so that vulnerable points of communication will not expose sensitive information for congruent systems within any given facility. Most technical standards are centric to IT networks only; therefore, there is a great need to re-think security from the current technological culture. Condortech Services, Inc. has brought together an integrated solution team made up of technology experts STT, LLC; Waverly Labs; SRC Technologies, Inc; and Senstar to mitigate and protect an entire Electronic Security System. A solution has to be approached through an integrated effort from multiple platforms and simultaneously has to begin exploring the use of advanced smart hardware.

The FFC's Cyber Resilience of Building Control Systems Workshop has acted as a touchstone for collaborative thought concerning the future security of Building Systems. As with the projected growth of the Internet of Things, government policy must move at break-neck speed to keep up with advances of the industry and the problem actors that prove to not only challenge the innovation, but also to pilfer and profit from it. Can we sit back and wait for the policy to materialize? Absolutely not! …as the FFC recognizes, representatives from the Security Industry, the BCS Industry and the associate government agencies that employ them must all come together to push forward the Cyber Initiative so that we can protect what has become the very core infrastructure of every physical facility with the Federal Government.

For further education about this event and to further explore any questions you may have concerning Cyber Resilience of Building Control Systems, please visit the following links:

Building Control Systems Cyber Resilience Workshop: *http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792*

Workshop Video Library: *https://vimeo.com/album/3689272*

Agenda with links to Presentations: *http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792#agenda*

PR Newswire article: *http://www.prnewswire.com/news-releases/condortech-services-inc-continues-commitment-to-protect-the-homeland-and-to-bolster-national-defense-through-cyber-security-awareness-at-building-control-systems-cyber-resilience-workshop-300208571.html*