OCTOBER 1, 2015

Rhode Island Cybersecurity Commission

Preliminary report to Governor Gina M. Raimondo per Executive Order 15-10: An initial action plan on steps the state can take to foster the resiliency of state government operations

Scott E. DePasquale
Chairman, Rhode Island Cybersecurity Commission

MEMBERS OF THE RHODE ISLAND CYBERSECURITY COMMISSION

EXECUTIVE BRANCH

Peter Gaynor, Director—Rhode Island Emergency Management Agency
Thom Guertin, Chief Digital Officer—Rhode Island Office of Digital Excellence
Macky McCleary, Director—Rhode Island Department of Business Regulation
Colonel Steven O'Donnell, Superintendent—Rhode Island State Police
Stefan Pryor, Secretary—State of Rhode Island Executive Office of Commerce
Colonel James Vartanian, Director of Plans, Operations & Training—Rhode Island National Guard

PRIVATE SECTOR

Gil Bishop, Chief Information Security Officer—Amica Mutual Insurance Company
Rear Admiral Michael Brown, USN (Ret), Vice President and General Manager, Global Public Sector—RSA
Matt Cullina, Chief Executive Officer—IDT911
Scott DePasquale, Chief Executive Officer—Utilidata *(Commission Chair)*
Stephanie Douglas, Senior Director of Corporate Security—Pacific Gas & Electric
Teresa Durocher, Vice President, Information Security—Citizens Bank
Suma Gaddam, Chief Information Officer—Care New England
Michael Gresh, Chief Information Officer—Electric Boat, General Dynamics
Brigadier General Jim Jaeger, USAF (Ret), Chief Cyber Services Strategist—Fidelis Cybersecurity
Molly Magee, Executive Director—Southeastern New England Defense Industry Alliance
Mark Munkacsy, Senior Engineering Fellow—Raytheon Integrated Defense Systems
Ray Musser, VP Global Security Operations (retired)—General Dynamics
Graham Wright, Chief Information Security Officer—National Grid

RHODE ISLAND ACADEMIC AND RESEARCH INSTITUTIONS

Chuck LoCurto, Chief Information Officer—Bryant University
Derek Reveron, Professor of National Security Affairs—U.S. Naval War College
John Savage, Professor of Computer Science—Brown University
Francesca Spidalieri, Senior Fellow for Cyber Leadership—Salve Regina University
Doug White, Director of Applied Networking and Security—Roger Williams University
Victor Fay-Wolfe, Director of Digital Forensics—University of Rhode Island

OTHER PUBLIC AND QUASI-PUBLIC AGENCIES

Vladimir Ibarra, Deputy Director—Providence Emergency Management Agency
Mark Levett, Chief of Strategic Partnerships Unit—Counterintelligence Division, Federal Bureau of Investigation
David Wilga, Vice President & Chief Technology Officer—Rhode Island Airport Corporation

For their significant leadership and contribution to the work of this Commission, special thanks to:

Senator Jack Reed, U.S. Senator for Rhode Island
Senator Sheldon Whitehouse, U.S. Senator for Rhode Island
Congressman James Langevin, U.S. Representative for Rhode Island's 2nd Congressional District
Congressman David Cicilline, U.S. Representative for Rhode Island's 1st Congressional District
Admiral James Stavridis, USN (Ret), Dean—The Fletcher School of Law and Diplomacy, Tufts University
Brigadier General Christopher Callahan, Adjutant General—Rhode Island National Guard
Lieutenant John Alfred, Officer-in-Charge, Computer Crimes Unit—Rhode Island State Police

TABLE OF CONTENTS

I. BACKGROUND

Ensuring resiliency in state government operations requires a multi-disciplinary approach to security. This has traditionally included training and skills development, the adoption of systemic processes that are flexible enough to address emerging and evolving threats, and investment in resources and technology. Cybersecurity adds a new dimension to this paradigm, which impacts almost every modality of government operations in the 21st century. Both the public and private sectors rely deeply on the vast array of connected networks that support everything from basic payroll processing, to much more complex methods of communications and data sharing. In addition, many processes that were once manual and offline are now automated and connected to the internet. As a result of this growing dependency on information and communications technology, state government operations are significantly more exposed to disruption than ever before. There is every indication that this reliance will continue to become more acute. The bottom line: the sensitive information that various state agencies store and the systems they rely on are becoming more and more susceptible to intrusions and access by unauthorized actors with malicious intent.

"There have been notable shortfalls in the use of detection and response processes and technologies."

In addition to the increasing exposure that state government operations have to networked information and communications systems, a 2015 PwC report on the *Global State of Information Security* indicates that data breaches and cyber-attacks are growing at unprecedented rates.[i] PwC reports that the total number of security incidents detected by respondents in the study climbed to nearly 43 million in 2014, up 48% from 2013, and the number of respondents reporting financial losses over $20 million doubled in the same period. PwC further reports that the compounded annual growth rate of detected cybersecurity incidents has increased 66% annually since 2009. Other concerning trends noted in the report include: (1) more breaches are reportedly from insiders, employees, and trusted third parties; (2) security spending and budgets are not keeping up with the increasing number of incidents; and (3) there have been notable shortfalls in the use of detection and response processes and technologies.

These statistics explain the threats and weaknesses that exist in both the public and private sectors. Worth noting is that public and private sector security are linked in many cases. For example, a 2015 Lloyd's Emerging Risk Report details the outcome of a simulation sponsored by the University of Cambridge that contemplated a wide scale cyber-attack on the U.S. power grid—which is operated by various private sector entities. The report predicts a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail, and chaos to transportation networks as infrastructure collapses.[ii]

The convergence of more reliance on connected systems with the alarming rate to which these systems are being exploited is leading to rapidly increasing costs and difficulty maintaining resiliency in state government operations—which can ultimately affect public safety directly.

Additionally, cybersecurity is not just relevant to information technology and network operations teams, but now affects directly the efficiency of state law enforcement, emergency response, and the National Guard. In fact, it is becoming clear that the unique landscape and reach of cyberspace will require states to play a more active role protecting and advancing our national security. These contributing factors have compelled many states to focus significantly on assessing and managing the digital risks to their borders, stakeholders, citizens, and the country. This is also the basis on which Governor Gina M. Raimondo established Rhode Island's first Cybersecurity Commission.

II. THE RHODE ISLAND CYBERSECURITY COMMISSION

The Rhode Island Cybersecurity Commission (Commission) was established on May 7, 2015 through Executive Order 15-10 and was charged with submitting an initial action plan by October 1, 2015 on steps that the State of Rhode Island should take to foster the resiliency of state government operations. The Commission consists of 28 members who come from state government, federal government, the private sector, and academia. The Commission was tasked to:

- establish a process to regularly assess cybersecurity infrastructure and activities within all executive branch agencies;
- identify awareness-training needs for state employees;
- pinpoint gaps and opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information;
- create a framework for coordinated responses, simulation testing, and mutual assistance by executive branch agencies and the private sector for cyber incidents; and
- examine best practices adopted by states around the country and evaluate whether or not they should be adopted in Rhode Island.

Five subcommittees were formed to develop an initial assessment of state operations, including:

- State Information Technology Systems Security Review Working Group;
- Rhode Island National Guard Development Working Group;
- State Police and Forensic Development Working Group;
- Information Sharing and Integration Center Development Working Group; and
- Workforce Development and Skills Training Working Group.

On July 16, the Commission kicked off its formal information gathering and analysis efforts with a Cybersecurity Summit at the U.S. Naval War College, bringing together experts from the government and private sector to discuss and educate stakeholders on emerging issues in cybersecurity and infrastructure resiliency. In the months that followed, the Commission conducted an analysis of relevant state agencies including the Rhode Island State Police, Rhode island National Guard, the Rhode Island Division of Information Technology, Rhode Island Emergency Management Agency, and the Rhode Island Fusion Center to assess their cybersecurity and information sharing capabilities, key challenges,

needs, gaps, and opportunities—as well as linkages between each of the agencies and with the private sector and academia.

The Commission was also tasked with reviewing opportunities to support the cybersecurity industry and workforce in Rhode Island, which will be presented in a follow-on report in December 2015.

III. EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

Early findings of the Commission suggest that Rhode Island is uniquely positioned to elevate its relevancy to the country's national security by improving integration and innovation across its cybersecurity assets. As outlined in further detail later in this report, Rhode Island has a strong cybersecurity ecosystem made up of key assets including:

- a strong congressional delegation with deep expertise in defense and cybersecurity;
- the U.S. Naval War College in Newport, Rhode Island;
- Rhode Island Air National Guard's 102nd Network Warfare Squadron and Rhode Island Army National Guard's Computer Network Defense Team;
- the Rhode Island Fusion Center;
- the Rhode Island State Police Computer Crimes Unit and digital forensics lab;
- a strong defense contractor community;
- a significant academic and research ecosystem; and
- a strong financial and healthcare driven private sector.

Despite these strengths, Rhode Island has not yet fully integrated and optimized its assets in a way that will ensure state government operations remain resilient. A number of consistent themes emerged throughout the Commission's interviews with Rhode Island state agencies and experts.

Theme 1: There is a lack of consistent coordination and information sharing across state agencies and core elements of the private sector. Without a more systematic, well-resourced process in place, it is unlikely that the state will be able to optimize its resources towards improved operational resiliency. Additionally, most key Rhode Island agencies lack the required budget to adopt best practices.

Theme 2: Within state agencies, private companies, and government offices, cybersecurity remains a secondary and adjacent effort, not fully integrated into core missions. Leaders across the state voiced their concerns that this approach is limiting the abilities of those charged with cybersecurity to ensure all aspects of an agency, company, and product are secure.

Theme 3: While state resources exist to help state agencies and the private sector train employees, address vulnerabilities, and tackle ongoing threats and attacks, there is a need for greater education and awareness about these offerings and expertise. Those in greatest need of these resources are often unaware of them.

Considering these and several other findings, the Commission compiled eight initial recommendations that, if implemented, would lead to a stronger foundation for operational resiliency within the state.

A summary of the initial recommendations include:

- **Establish a strategic leadership role for cybersecurity that is integrated into the Homeland Security mission for the state and is directly accountable to the Governor:** Hire executive leadership to better foster strategy, leverage state assets, oversee ongoing security integration between state and federal agencies, and sponsor nationwide relationships with key stakeholders. The state should also consider establishing a homeland security advisory board with national level expertise in cybersecurity to support the new office. It will be critical for this role to be fully integrated into the broader homeland security activities of the state—which are currently under-developed.

- **Improve statewide executive branch cyber-hygiene, skills training, risk management, and technology deployment:** The state should upgrade its tools and risk management processes to be consistent with best practices for state network operations. This should include adding human resources dedicated to cybersecurity within the Division of Information Technology itself, acquiring advanced real-time network monitoring sensors and capabilities such that the state networks can be systemically assessed, and rolling out system-wide training to all state employees on cyber-hygiene—focusing on spear phishing in particular. The Division of Information Technology should also adopt a robust risk based approach to security strategy.

- **Upgrade the state's existing Cyber Disruption Team to create a more enhanced cybersecurity response, outreach and training capability for Rhode Island stakeholders:** Better integrate the State Police, National Guard, Division of Information Technology and other state resources to create a *Joint Cyber Task Force* comprised of dedicated full and part-time local, state and federal resources with military, academia and emergency management expertise. The Joint Cyber Task Force should be used for training and support in addition to the current response mandate of the Cyber Disruption Team—and should co-locate its operations with the Rhode Island Fusion Center. This task force will need to develop an improved set of protocols, commitments, and a conception of operations that reflects its expanded mission and integration into Fusion Center activities.

- **Expand the Rhode Island Fusion Center to better integrate existing state and federal law enforcement, intelligence, defense, emergency response, and critical infrastructure protection operations:** Through an enhanced Fusion Center architecture, Rhode Island could set the standard for other states in the application of best practices for cybersecurity with a multi-faceted approach that contemplates strategy, technology, and forensic capabilities—all of which must be incorporated directly into the law enforcement and intelligence missions. In order to advance resiliency related to cyber, the state must unify and better integrate its existing capabilities to include co-location of the State Police Computer Crimes Unit, digital-forensics lab, the National Guard, and select members of the private sector with the Fusion Center. This will require re-locating the existing Fusion Center

to a larger dedicated facility—while maintaining the current partnership and co-location with the Federal Bureau of Investigation (FBI).

- **Improve the Rhode Island National Guard's [Air National Guard's 102nd Network Warfare Squadron and Army National Guard's Computer Network Defense Team] connectivity with U.S. Cyber Command and the 24th Air Force:** Establishing joint training exercises for Rhode Island soldiers and airmen through rotational stations at both Fort Meade and Joint Base Lackland could seed longer term opportunities to further develop force structure. The training and skills development gained could greatly benefit Rhode Island stakeholders—particularly given the significant role that the National Guard plays in the Rhode Island Cyber Disruption Team (and proposed Joint Cyber Task Force).

- **De-constrain the Rhode Island Air National Guard's cyber resources:** Rhode Island leadership should play an active role supporting the policy work being done by the Department of Defense such that the Rhode Island National Guard can be more effectively deployed in support of the state's rapidly evolving cybersecurity needs. In the interim, a clear set of expectations should be set under which Rhode Island National Guard resources can be activated and deployed to combat emergent cyber threats and vulnerabilities. These resources could play a significant role in helping various state entities assess and mitigate network security threats—which are becoming significantly more persistent and pervasive.

- **Establish an enhanced cyber-forensic development plan within the Rhode Island State Police that promotes best-in-class capabilities:** Continue to develop and enhance working relationships between the State Police senior leadership and the FBI, the National Counter Intelligence and Security Center, and Department of Homeland Security senior leadership (among others). The aim is to improve exposure to partnering and federal grant opportunities. The State Police will need to further recruit both sworn officers and civilians with the appropriate technical backgrounds to address the rapidly evolving need for digital expertise, as there is currently a deficit of these resources within the agency (particularly the shortage of malware reverse engineering capabilities). Additional human resources and cyber-forensics will be needed in the near-term to address the growing number of cyber-incidents that the State Police are required to respond to.

- **Further assess and develop a framework for establishing a Rhode Island based National Cyber Center of Excellence:** State leadership should look for opportunities to build upon the significant simulation and war-gaming capabilities within the U.S. Naval War College, the newly proposed Joint Cyber Task Force, and an expanded Fusion Center. A more refined partnership structure between the state and its federal, local, academic and private sector partners could be a long-term catalyst and focus area for both security and economic development within Rhode Island.

IV. STATE OF THE STATES FOR CYBERSECURITY

Cybercrime now ranks as the top national and economic security threat facing our country—ahead of terrorism, espionage, and weapons of mass destruction.[iii] As cyber threats grow in scope and sophistication, the federal government has worked to develop appropriate standards, policies, and regulations. However, cybersecurity cannot be tackled at the federal level alone. States have a responsibility to secure their critical infrastructure as well as the data that has been entrusted to them by their citizens.

"Cybersecurity cannot be tackled at the federal level alone. States have a responsibility to secure their critical infrastructure as well as the data that has been entrusted to them by their citizens."

In recent years, six states have made particularly noticeable strides in addressing cybersecurity issues by crafting innovative solutions that improve resiliency and creatively turn cybersecurity challenges into opportunities. The unique advantage of these six states—Maryland, Texas, California, Virginia, Idaho, and Rhode Island (a detailed report on Rhode Island's cybersecurity assets can be found in Section V)—is that they have launched formal cybersecurity commissions, councils, or task forces designed to strengthen their cybersecurity posture. Each has made recommendations to their governors and state agencies to improve preparedness, resiliency, response capabilities and support for the growth of their cybersecurity industry and workforce.

Maryland

Maryland has effectively leveraged its existing assets, proximity to the federal government, and strong leadership to stand up the first National Cybersecurity Center of Excellence—branding itself as the cybersecurity "epicenter" of the country.

Resources: Maryland benefits from being home to highly relevant cyber resources such as the Defense Information System Agency (DISA), the National Security Agency (NSA), United States Cyber Command, the National Institute of Standards and Technology (NIST), the University System of Maryland, various cyber incubators and startup companies, and strong leadership at the gubernatorial and congressional level. This ecosystem of stakeholders was instrumental in creating the Maryland Commission on Cybersecurity Innovation and Excellence, which was tasked with the development of comprehensive, coordinated, and rapid response strategies to proactively protect the state from cyber-attacks, while promoting cyber-innovation and job creation.

Initiatives: Maryland's collaborative approach to managing its stakeholders allowed the state to set the precedent in public-private cybersecurity partnerships. In collaboration with the U.S. Department of Commerce's NIST, Maryland created the first National Cybersecurity Center of Excellence (NCCoE), bringing together industry, academia, and government experts to provide businesses with cybersecurity solutions based on commercially-available technologies.[iv] In addition, the NCCoE established a Federally Funded Research and Development Center (FFRDC) which is operated by the MITRE Corporation. The

FFRDC is committed to supporting the work of the NCCoE and developing practice guides to aid industry in adopting standards-based approaches to tackle cybersecurity challenges. With the FFRDC capabilities, Maryland's NCCoE has become a powerful centerpiece in attracting millions of federal dollars and new businesses to the state. This new hub for innovation and development in Maryland now serves as a testing ground for users and vendors to collaborate on new ideas and technologies.

With a powerful testbed foundation in place, the NCCoE launched the National Cybersecurity Excellence Partnership (NCEP), which facilitates the collaboration of U.S. companies interested in joining their cyber efforts. Partners include Cisco, Intel, McAfee, Microsoft, RSA, and Symantec—among several others. Additionally, Maryland launched the CyberMaryland initiative to bring together entrepreneurs, investors, academia, private enterprise, and government officials, further reinforcing the state's leadership in cybersecurity and information technology.

Legislation: The Maryland Commission was successful in proposing and supporting the passage of cybersecurity-related legislation, including:

- a law that allows for provisions to protect executive state agency databases against cyber-attacks and requires citizens to be notified when personal information is compromised; and
- expanding the identity theft statute to include health care information, allowing for the prosecution of those crimes, and enabling victims to more effectively seek restitution.[v]

Additionally, former Governor Martin O'Malley approved a Cybersecurity Investment Incentive Tax Credit, which provides refundable income tax credits to qualified Maryland cybersecurity companies that demonstrate an ability to secure private investment capital.[vi]

Texas

Texas relies on the Texas Cybersecurity, Education, and Economic Development Council (Council) and the Department of Information Resources (DIR) as the primary drivers for state-wide cybersecurity initiatives.

Initiatives: The Council was created in 2011 to provide recommendations to state leadership on steps that can be taken to improve critical cyber infrastructure and accelerate growth within the cybersecurity industry in Texas. When the Council published its first report in 2012, there was not a single lead office in the state responsible for the coordination of cybersecurity policy and response. The Council made several recommendations in 2012, establishing a framework for statewide action on cybersecurity. Although not all of the Council's recommendations were implemented, they have helped streamline cybersecurity best practices across the state, encouraged investments in cybersecurity programs, and promoted collaboration and entrepreneurship within the state's cyber environment. Recognizing that the Texas Department of Information Resources (DIR) had established a strong information security program for state agencies—the Council recommended that DIR's duties and powers be expanded. The DIR now provides various security services to state agencies and higher education institutions—which

allows it to operate as a self-funded agency. Within the DIR, the Cybersecurity Coordinator, who is also the state's Chief Information Security Officer, has authority to establish standards and enforce compliance to those standards within the various state agencies.

In an effort to create jobs and develop a well-trained talent pool of cybersecurity professionals, the Cybersecurity Coordinator has established the Texas Business Council (TBC)—which supports public-private partnerships, aligns competencies, and creates mutually reinforcing incentives for both companies and universities. Additionally, DIR has created the Texas InfoSec Academy, an educational program specifically designed to train security professionals within the state on incident handling, forensics, disaster recovery, and network penetration testing.

In an effort to increase communications and response between state government entities, the DIR is developing a Governance, Risk, and Compliance (GRC) portal for its agencies. The GRC will go beyond reporting raw security incident data, and will provide real-time actionable analysis, comparable statistics for incident management and response, and more effective management protocols during the investigation process.[vii] This enhanced incident response process will assist the efforts of the Texas Emergency Management Agency, DPS, and other key state agencies in their ability to improve law enforcement efforts when a cyber-incident occurs.

Finally, in September of 2015, the Department of Homeland Security awarded the University of Texas at San Antonio an $11 million grant to develop information sharing standards—allowing the University to support the public and private sector in establishing Information Sharing and Analysis Organizations.

California

In light of creating the first state-led cybersecurity task force, California is leveraging its Silicon Valley ecosystem, universities and research institutions to establish its reputation as the "test state" for all things cyber.

Resources: The Silicon Valley technology eco-system provides a potential gold-mine of talent and resources, helping the state establish itself as a leader in cybersecurity. However, there exists a cultural disconnect between Silicon Valley and the public sector—particularly the intelligence community. California is taking steps to improve collaboration opportunities with the Silicon Valley community, which will help the state better access the benefits of its rich talent pool.

Initiatives: California launched the first state-led collaboration of its kind with the creation of the California Cybersecurity Task Force (Task Force) in 2013—which was a response to Presidential Executive Order 13636 on Improving Critical Infrastructure Cybersecurity.[viii] The Task Force is made up of over 120 members from state, local, federal and tribal government, research, academia, and private industry. The strategic objectives of the California Cybersecurity Task Force include:

- identifying areas where stakeholders can improve statewide collaboration and information sharing to identify potential threats;
- developing strategies for threat prevention, remediation, response, and recovery;
- reviewing areas where coordination will enhance security, emergency response, communications, and contingency planning across the state of California; and
- conducting public outreach and awareness of cybersecurity as a priority.[ix]

While the California Cybersecurity Task Force has made great strides in its approach to safeguard both information and infrastructure within the state, progress and implementation has been slow since 2013.

Legislation: California was the first state in the country to require data breach notifications. The State set a clear course of action for businesses to follow in the event of a network compromise—including reporting of data breaches to the Office of the Attorney General, the State Police, and the Department of State. Governor Jerry Brown recently signed an executive order that outlines ways to bolster California's preparedness and response to destructive cyber-attacks—including the creation of a California Cybersecurity Integration Center (Cal-CSIC), which will be responsible for strengthening the state's cybersecurity strategy and improving inter-agency, cross-sector coordination.[x] Cal-CSIC will work closely with the California State Threat Assessment System and the U.S Department of Homeland Security to facilitate more integrated information sharing and communication with stakeholders in the state. Under the executive order, Cal-CSIC will establish a multi-agency Cyber Incident Response Team responsible for coordinating threat detection, reporting, and response with public and private entities across the state.

Virginia

Virginia, like Maryland, has leveraged its proximity to the federal government, business-friendly policies, and existing partnerships with local companies and universities to promote cybersecurity innovation and attract significant federal investments for its research and development institutions.

Initiatives: In 2014, Virginia Governor Terry McAuliffe established the Virginia Cybersecurity Commission (VCC) to identify high-risk cybersecurity issues facing the Commonwealth of Virginia, provide suggestions for more secure network plans and procedures, offer response strategies and best practices for the state, promote cyber hygiene, help facilitate the development of cutting-edge science and technology in the cybersecurity realm, implement state cyber assessments, and contribute to the overall cyber-safety of Virginia stakeholders.[xi]

The VCC established a Cyber Crime Working Group which is responsible for reviewing state statutes that govern cybercrimes, providing recommendations for legislation to update the definition of what constitutes a “cyber-crime”, and improving the capabilities of law enforcement in investigating such crimes. Members of the working group include the Virginia State Police and the High Tech Crimes Division, which is the primary state authority in charge of investigating and conducting forensics analysis of computer crimes.

Virginia also established a Cybersecurity Partnership comprised of public and private sector cybersecurity professionals to promote mutually beneficial information sharing and to foster workforce development.[xii] In addition, not only is Virginia in the process of establishing the first-of-its-kind state Information Sharing and Analysis Organization (ISAO),[xiii] it was the first state to adopt the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Legislation: The Virginia Commission has identified, reviewed, and updated important cybersecurity related bills and was instrumental in supporting their passage with the Virginia state legislature, including:

- a bill requiring each state agency to be responsible for securing its own electronic data;
- a law to help verify and authenticate an individual's identity online;
- a law providing wider authority to the Attorney General in investigating crimes involving pornography, abduction, or prostitution; and
- updates to the Virginia Freedom of Information Act that support protecting sensitive security related information as an exception to open meeting requirements.

Finally, Governor McAuliffe has recently issued a new executive order mandating a strategic plan to address data security across state government. The executive directive requires the Virginia Information Technologies Agency (VITA) to review the state's risk management capabilities and to provide recommendations for strengthening how the state addresses cybersecurity issues. The order also calls for VITA to conduct agency audits and present a status report in 2016.[xiv]

Idaho

Most recently, Governor C.L. Otter created the Idaho Cybersecurity Task Force to develop policies, programs, and strategies to detect vulnerabilities and prevent cyber-related attacks within the state.

Initiatives: The Governor's Executive Order was driven by cyber incidents that directly targeted the Idaho Supreme Court's website in 2014 and the server of a state agency website in 2015.[xv] Governor Otter also asserted that the state's economic competitiveness is correlated to its degree of cybersecurity, therefore justifies the need for further state action. The Idaho Bureau of Homeland Security used the Executive Order to initiate the Idaho Interdependencies Workshop, bringing together relevant constituents across multiple sectors from the state. The participants of this workshop included the Idaho National Laboratory, Micron Technology, Hewlett-Packard, St. Luke's Health System, Supervalu Inc., Boise State University, Norco, the City of Boise, and sheriff's offices statewide.[xvi] This Workshop led to the creation of the Cybersecurity Task Force—which first convened in September.

Other States Initiatives

While the majority of states have not yet established formal cybersecurity commissions of their own, the innovative and progressive actions that a few other states have taken in this area are noteworthy.

- **Michigan** is the only state that has had a dedicated Cyber Security Strategic Plan since 2009, part of its overall Michigan Cybersecurity Initiative. It was also the first state to create a Chief Security Officer Position responsible for both physical and cybersecurity. In addition, Michigan has developed a sophisticated system for early detection and rapid response—which includes State Police, the Michigan National Guard, Emergency Management, and the Michigan Cyber Civilian Corps—whose members play a key role in Michigan's comprehensive Cyber Disruption Response Strategy.

- **Washington** was one of the first states to use the National Guard in a cybersecurity capacity. Deployed in "Red Team" exercises, the Governor has used the National Guard to evaluate the strength of Washington's networks and to conduct cyber-emergency planning. Similarly, senators from New York and New Jersey have proposed the creation of a joint State National Guard Cyber Protection Team capable of addressing the increase in cyber-threats focused on network infrastructure in the region.[xvii]

- **New York** has designed specific report cards for state agencies so the state can conduct self-assessments and measure their compliance against specific security standards. It has also been able to develop an effective partnership with the FBI, the local Department of Homeland Security investigative branch, and the state and local police to combat cyber threats. After September 11, 2001, New York was among the first to recognize the importance of information sharing and connecting different sectors to efficiently assess, prioritize, defend against, and respond to physical and cyber threats.

- **New Jersey** launched the first-of-its-kind New Jersey Cybersecurity and Communications Cell (NJCCIC) as a central state civilian interface for coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors.[xviii] California is now in the process of establishing a similar agency.

V. STATE OF RHODE ISLAND – KEY AGENCY CAPABILITIES

It is vital for leaders in Rhode Island to proactively address the growing number of cyber-based threats. Not only to mitigate state network vulnerabilities, but as part of the state's overall responsibility to enhance law enforcement capabilities, private sector integrity, and ultimately our country's national security. As cyber threats continue to grow in scope and complexity, state government also has the difficult task of securing its critical infrastructure and the significant amounts of public data entrusted to it. Key state agencies must play a fundamental role in reducing risks, increasing operational resiliency, and ensuring that their organizations are appropriately resourced to support these endeavors.

The Rhode Island State Police and its Cyber Disruption Team, Fusion Center, Rhode Island National Guard, Rhode Island Emergency Management Agency, and Rhode Island Division of Information Technology collectively possess valuable capabilities that can be applied to combating advanced

persistent cyber-threats. These agencies will need to effectively collaborate, train, respond, and manage change across all of the dynamic elements related to cybersecurity.

The Rhode Island Division of Information Technology

The Rhode Island Division of Information Technology (DoIT) plays a critical role securing state agency networks, protecting data, and responding to computer and network attacks.

Current Capabilities: DoIT is responsible for managing the network and security enterprise for state executive branch agencies, public universities and colleges, and a number of satellite locations that serve the State of Rhode Island. Network traffic is managed across multiple providers to ensure that performance, reliability, and redundancy are maintained in day-to-day operations. The network features a number of primary and secondary sites with direct links in place to handle interagency needs, as well as multiple data centers hosting internal and external applications. DoIT has deployed a number of solutions across the network to strengthen the security and privacy of systems, data, and transmissions wherever required. In addition, DoIT has implemented a framework to detect and prevent intrusion, as well as secure physical access to sensitive locations.

DoIT supports the state's network and cybersecurity efforts with a small group of technology professionals who are well versed in cybersecurity measures and actions. These personnel resources, however, are not fully dedicated to this work. The existing methods that DoIT uses to protect the state's network operations should be modernized and enhanced through the deployment of proper training, technology, and additional man power. DoIT has made significant investments in state-of-the-art firewalls, network monitoring, hardware and software, third party assessments, and regular internal penetration testing. However, DoIT is in need of a number of upgrades to its software and hardware—and does not have the necessary network monitoring tools to fully assess traffic and conduct expert research and analysis on suspected issues in real-time. More robust processes, national standards and a risk based model for cybersecurity should be adopted.

Recommendations: The following recommendations are focused on enhancing current network and systems security:

- ensure that a robust real-time network monitoring capability is deployed and staffed with human resources dedicated to assessing daily threat data;
- develop a cybersecurity training platform for all state employees—particularly addressing the need to regularly educate all system-users on proper cyber-hygiene and spear-phishing—*mandated annual cybersecurity training and certification should be in place for all employees and contractors before allowing access to computers and the state network;*
- incorporate advanced training in threat detection and mitigation, network analysis, and the latest security protocols for all key employees of DoIT;
- engage a qualified independent firm to conduct annual security audits and third party network penetration testing;

- conduct a review with the Bureau of Audits to inventory and assess whether or not all information technology policies are current;
- update and revise purchasing rules to allow for the trial and deployment of software and hardware in an expedited manner;
- create an inter-agency working group to improve policies and procedures for the destruction of data, hardware, and e-media—*existing policies are not consistent across all agencies, quasi-public entities, and third party providers;*
- update standard contracts with service and technology providers to ensure that the state is safeguarded against exposure from unsecure third party implementations;
- assess the potential migration of all state agency websites to a more secure environment; consider options that isolate public traffic and prevent unwarranted network access; and
- develop stronger partnerships with both internal and external entities through the proposed Joint Cyber Task Force.

Existing DoIT policies may not adequately address data protection and cyber defense. Many of the policies need to be modernized—accounting for new methods and approaches that have been automated by technology over the last decade.

The Rhode Island State Police

The State Police have a proven track record of addressing cybersecurity issues across the Ocean State. With targeted efforts underway, and experts within the department, the State Police have built a strong foundation to support operational resiliency and the law enforcement mission in Rhode Island.

Current Capabilities: The Rhode Island State Police operate two teams that deal with cyber-related incidents: (1) the Computer Crimes Unit; and (2) the Cyber Disruption Team.

The Computer Crimes Unit (CCU) is responsible for managing all criminal digital forensics for state and local police departments in Rhode Island. The CCU consists of nine full and part-time local police members and two federal agents that are members of the Rhode Island Internet Crimes against Children Task Force. With limited resources, the Computer Crimes Unit handles an increasing number of forensic examinations every year. For example, in 2014 the group received 926 requests for cyber or digital-forensic support, up from approximately 634 in 2013. Members of the CCU are also responsible for civic outreach, training, breach response, executing warrants for arrests, and conducting digital forensics associated with casework. Due to the increase of malicious cyber activity and the increased need for forensic examinations, additional personnel are needed to meet the demands of current cases, provide expertise and response capabilities, and to prosecute the growing number of cyber-crimes.

Separately, the Rhode Island State Police Cyber Disruption Team (CDT) was formed in 2009 as a collaborative effort between the Rhode Island State Police and the Rhode Island Emergency Management Agency. The CDT has now served for more than six years as an important extension of the

Rhode Island State Police Computer Crimes Unit—tasked to address the growing need for a quick response capability on incidents that threaten the state's critical information and communications infrastructure. The CDT provides analysis and support prior to and during cyber incidents affecting critical cyber-infrastructure in Rhode Island. This team can be deployed in support of operational continuity and the restoration of various system and network operations within the state. The team regularly conducts outreach and training exercises for its members, which meet bimonthly to exchange information. The members of the CDT can also share sensitive information and intelligence using a secure portal under the Homeland Security Information Network.

The group serves as an important vessel to which the State Police can organize and deploy cyber-resources from various local public and private sector organizations—including the Rhode Island National Guard, Division of Information Technology, Emergency Management Agency, as well as members of the local business and academic community.

Recommendations: Re-establish the Rhode Island Cyber Disruption Team as the *Joint Cyber Task Force*. The Joint Cyber Task Force would utilize the same human resources from multiple public and private sectors to provide robust protection and response to wide-spread cyber-disruptions. However, some critical changes and recommendations include:

- expand the group's mission to include support for casework within the State Police Computer Crimes Unit and outreach, education and training for Rhode Island's public and private sector stakeholders (including small to medium size businesses);
- further integrate relevant cyber capabilities from the State Police, National Guard, Division of Information Technology, Emergency Management Agency, academia, and the private sector to create a more enhanced task force of dedicated full and part-time personnel;
- integrate the group's physical location and activity directly into Rhode Island Fusion Center operations—consider co-locating the State Police Computer Crimes Unit and forensics lab;
- develop an improved set of protocols, commitments, and a conception of operations that reflect the expanded mission and duties;
- develop an operating structure that will allow the task force to systemically disseminate current and imminent threat indicators to state, city and town agencies, as well as participating members of the private sector; and
- develop an active liaison program for state, federal, military, private, and academic resources to facilitate joint exercise and training opportunities.

By making the appropriate investments in trained, multidisciplinary personnel, the Joint Cyber Task Force can provide resources that are flexible and responsive to the growing threats in cybersecurity. Dedicating personnel to specific missions of defense, response, forensic analysis, information sharing, training, and education can significantly enhance the resiliency of state government operations. The Joint Cyber Task Force should remain accountable to the Superintendent of the Department of Public Safety, who is also the state's Homeland Security Advisor. Additionally, the task force will require a Director that can provide leadership on cybersecurity operations, intelligence and best practices.

The Rhode Island National Guard

The Rhode Island National Guard (Guard) plays a critical role in supporting the state's cybersecurity efforts despite the Federal restraints it currently operates under.

Current Capabilities: The Guard has substantial capabilities related to detecting, analyzing, and researching network intrusions and vulnerabilities—primarily through the Rhode Island Air National Guard's 102nd Network Warfare Squadron (NWS) and simultaneously through the Rhode Island Army National Guard's Computer Network Defense Team (CND-T). These Guard units house a significant number of citizen airmen and soldiers with skills and capabilities that can support table-top simulation exercises, cyber range training, risk analysis, compliance assessments, network intrusion detection, network intrusion response, digital forensics, technical testing, ethical hacking, and technical reporting and briefing. In addition, the Guard can offer information security and cyber planning in support of various public and private stakeholders in Rhode Island.

While the Guard is well-positioned to leverage its capabilities to help prevent, protect, respond, mitigate, and recover from a cyber-incident against the state—significant federal policy changes would be required to allow Guard personnel to more effectively engage with both the public and private sector stakeholders. Department of Defense (DoD) policy and legislative barriers are constraining the Guard's ability to fully integrate cybersecurity resources—limiting their activity in normal operating conditions to an advisory, training, and assistance role. As a start, the creation of the proposed *Joint Cyber Task Force* would allow the Guard a platform to better mobilize its resources for the benefit of state government and private sector.

Recommendations: Broadening the mission of the 102nd Network Warfare Squadron and its exposure to the Department of Defense, United States Air Force, and U.S. Cyber Command can yield substantial benefits to the State of Rhode Island in the future. Those benefits include an enhanced ability for the Guard to yield an increased amount of well-trained human resources to the state's cyber-stakeholders for training, assessment, and response. The following recommendations support those efforts:

- assess the 102nd Network Warfare Squadron's future mission opportunity within the U.S. Airforce—this may impact relevancy and future force structure;
- expand regular interactions between the Guard and U.S. Cyber Command at Fort Meade; look for opportunities to co-locate a select group of airmen and soldiers with U.S. Cyber Command and the 24th Air Force in San Antonio;
- support ongoing efforts at the National Guard Bureau to allocate additional funds to the Rhode Island Army National Guard's Computer Network Defense Team—as these resources could benefit Rhode Island stakeholders;
- work closely with the National Governors Association (NGA) to leverage Rhode Island's cybersecurity assets at the national level—look for additional grant funding opportunities and participation in nation-wide cyber-exercises
- the Guard should review and revise the Memorandum of Understanding for its participation

in the CDT (to be Joint Cyber Task Force) with the State Police to reflect a more cohesive, effective, and efficient cybersecurity capability and mission set for the defense of the state.

Of note: on February 16, 2016 the Department of Defense will publish a draft policy addressing the use of the National Guard by states in the event of a cyber-attack—which could influence homeland security legislation to include an enhanced role for the Guard in cyber defense.

Lastly, in its efforts to support the development of cybersecurity infrastructure and programs in the State of Rhode Island, the Guard must exercise caution when using federal funding to support state missions, as this can lead to purpose violations when not assessed and executed appropriately.

The Rhode Island Emergency Management Agency

The Rhode Island Emergency Management Agency (RIEMA) plays a critical role in both cybersecurity policy setting and the coordination and integration of state resources for cyber-incident response.

Current Capabilities: The mission of RIEMA is to reduce the loss of life and property for natural, technological, and man-made incidents. In order to achieve this mission, RIEMA utilizes an all hazards approach to preparedness, response, recovery, and mitigation—while providing leadership, assistance, and support to regional, state, tribal, and local entities. Infrastructure protection is a continuous process with many intersecting elements and interdependencies that cross jurisdictions and natural boundaries. Protecting critical infrastructure from all hazards is an essential first step in building a resilient cybersecurity enterprise within the state. RIEMA works proactively with key stakeholders to address the persistent cybersecurity risks that threaten Rhode Island. As a core member of the Cyber Disruption Team (CDT), RIEMA is responsible for:

- coordinating with specifically identified emergency support functions during an activation;
- identifying Critical Infrastructure and Key Resources (CIKR) within the State of Rhode Island;
- requesting the issuance of a state of emergency declaration through both the Governor's Office and the Federal Emergency Management Agency;
- assisting in the restoration of communications and infrastructure;
- coordinating federal support; and
- providing state-wide damage assessments to the Governor.

During a cyber incident, the CDT will report information to RIEMA and the Rhode Island Fusion Center. Working within the Fusion Center, RIEMA's Critical Infrastructure Protection Coordinator is tasked with identifying and assessing the state's critical infrastructure priorities. Within the Rhode Island Critical Infrastructure Program, an enhanced security and resiliency strategy for CIKR has been established for state agencies to follow—which outlines the information required to understand security needs, identify vulnerabilities, and to develop executable sector-specific plans. The Rhode Island CIKR program follows a nationally developed set of priorities originally outlined in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.

Additionally, RIEMA has developed the Cybersecurity Protection Program. This program was designed to assist organizations in mitigating cybersecurity risks by providing practical guidelines to protect against and detect malicious activity and respond to incidents. Within the Cybersecurity Protection Program, plans and policies have been drafted to improve cybersecurity across the state enterprise–and are based on recommendations from the National Institute of Standards and Technology (NIST). The draft plans and policies include:

- the Rhode Island Cybersecurity Protection Plan—based on the NIST Framework;
- the Rhode Island Cybersecurity Incident Action Plan—based on NIST Special Publication 800-61; and
- 40 additional cybersecurity policies—all based on NIST Special Publication 800-150.

Also part of RIEMA's Cybersecurity Protection Program is the Cyber Range Program. The Cyber Range Program fosters whole community engagement by promoting a unique, hands-on testing environment in which virtual elements are subjected to numerous simulated internal and external conditions that individuals can train against. Following the purchase of the state-of-the-art Cyber Range, RIEMA has been collaborating with the Community College of Rhode Island to create an innovative training program—providing individuals with the opportunity to use the Cyber Range to acquire the knowledge and skills necessary to advance their cyber defense capabilities. The Cyber Range Program is expected to serve as a platform for developing enhanced cyber-skills and workforce education within the state—which if scaled can significantly contribute to better cyber-infrastructure protection for Rhode Island.

Recommendations: While RIEMA is engaged and investing in infrastructure protection and cybersecurity, there are a number of issues hindering the agency's ability to provide leadership, assistance, and support to Rhode Island. Key recommendations include:

- creation of a working group to assess the state's current homeland security model, and potential need for a statue that clearly outlines roles, responsibilities, and priorities to cover security coordination throughout all of state government;
- development of an overarching Rhode Island Cybersecurity Strategy that outlines the requirements for doctrine, policies, procedures, and how the state will defend networks, systems, and information against priority threats; and
- an executive order requiring state agencies to recognize and adopt the Rhode Island Cybersecurity Protection Plan, the Rhode Island Cybersecurity Incident Action Plan, and the 40 draft policies developed by RIEMA (all based on NIST standards)—RIEMA should develop a systematic process to regularly exercise these plans for relevancy and usefulness.

RIEMA is well positioned to support key state-wide cybersecurity strategies, and is currently managing most interactions with DHS in support of funding and grant opportunities for cyber-stakeholders within the state. However, a permanent state funding mechanism is needed to finance ongoing strategic cyber-operations.

The Rhode Island Fusion Center (RIFC)

State Fusion Centers were established across the nation following September 11, 2001 as part of a comprehensive Homeland Security and Public Safety Program developed by the U.S. Department of Homeland Security. Fusion Centers serve as focal points within state and local environments for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial and private sector partners. Accordingly, the Rhode Island Fusion Center (RIFC) was established in 2005 to assist state, local and regional law enforcement and public safety operations in the collection, evaluation, and dissemination of actionable intelligence.

"These threats now range from the Islamic State of Iraq and the Levant (ISIL), to localized threats such as home grown violent extremists and other universal threats across the virtual or cyber domain."

The threats that brought about fusion centers have grown and evolved significantly to include global acts of radical idolized violence. These threats now range from the Islamic State of Iraq and the Levant (ISIL), to localized threats such as home grown violent extremists and other universal threats across the virtual or cyber domain. Fusion centers, including the RIFC, must constantly adapt to combat these evolving threats.

Current Capabilities: The RIFC is led and staffed by the Rhode Island State Police, supported by local police officers, a Department of Homeland Security intelligence analyst, and emergency management professionals. Since its inception, the RIFC has shared its space with the Federal Bureau of Investigations' Providence Resident Agency, which includes the Joint Terrorism Task force (JTTF). Other RIFC and state homeland security resources include:

- the RI State Police Computer Crimes Unit (CCU)—also led and staffed by the Rhode island State Police and supported by local police officers;
- the Rhode Island Cyber Disruption Team (CDT), which serves as the state's incident response team in the event of a significant cyber-disruption event or incident. The CDT is comprised of law enforcement, IT professionals, and emergency managers; and
- a Rhode Island Emergency Management Agency employee assigned to the RIFC with the goal of improving information sharing for "all-hazard" threats, synchronizing the state's Critical Infrastructure and Key Resource (CIKR) objectives, and integrating relevant members of the newly formed RI Business Alliance (RIBA).

The Rhode Island CIKR Program was designed to ensure that the state maintains the capabilities necessary to save lives, protect property and the environment, and to meet basic human needs after an incident has occurred. Meanwhile, the mission of the RIBA is to integrate private sector services and government resources to capitalize on the collective knowledge base. Though challenged by geography,

all the above mentioned agencies cooperate daily, through multiple modalities and from numerous offices located across the state.

Recommendations: The RIFC architecture should be restructured to reflect a mutually supporting, fully integrated information sharing hub that is able to provide relevant and actionable intelligence in a timely manner to prevent, mitigate, and respond to emergent threats. Recommendations include:

- better integration of leadership from various state agencies into the RIFC. While day-to-day operations of the fusion center should be governed by the State Police—further integration of public and private sector partners will increase the depth and reach of the state's homeland security function.
- incorporate the Department of Justice Anti-Terrorism Advisory Council and an intelligence analyst from the Rhode Island National Guard—the goal is to vertically and horizontally integrate both state and local law enforcement, FBI, DoJ, DoD, DHS, emergency management, and public-private partners;
- realign the Cyber Disruption Team into the proposed Joint Cyber Task Force—which will now serve as the state's cybersecurity hub for indications and warnings on threat data; and
- consider co-locating the State Police Computer Crimes Unit and forensic lab with the Fusion Center.

The RIFC should collect information using an all-crimes approach—converting collected information into operational intelligence, and disseminating that intelligence in an effort to prevent acts of terrorism, cyber-attacks, and crime. The RIFC can be a model for fully integrating the collection, analysis and dissemination of criminal, terrorism, cybersecurity and all-hazard threat intelligence affecting or having the potential to affect Rhode Island, New England, and the nation.

VI. PREAMBLE TO DECEMBER REPORT—INDUSTRY AND WORKFORCE DEVELOPMENT

In addition to assessing the resiliency of state government operations, Executive Order 15-10 calls for the Commission to present an action plan outlining steps the state should take to support the growth of a cybersecurity industry and workforce by December 1, 2015. As part of that effort, the Commission will (1) conduct an assessment of the current cybersecurity workforce development and education activities within the state; (2) inventory existing businesses in the cybersecurity industry within the state; (3) survey institutions of higher education on cybersecurity related research and development activities; (4) determine barriers to expand workforce and business development opportunities and provide recommendations on eliminating those barriers; and (5) examine best practices around the country related to economic development within cybersecurity and evaluate whether or not they should be applied in Rhode Island.

The Commission will sponsor a Cybersecurity Summit on October 15, 2015—focusing on the future role of innovation, technology, and research—with several industry leaders and academic institutions participating.

VII. ANNEX 1—LIST OF RHODE ISLAND CYBERSECURITY SUBCOMMITTEES

Subcommittees Related to Resiliency of Operations
Steps the State should take to foster the resiliency of State operations

1. State IT Systems Security Review Working Group

A high level operational baseline of the digital and IT infrastructure supporting executive branch agency operations needs to be developed. This exercise should focus on level-setting the current state of risk management practices, policies, vulnerabilities, and the resiliency of network operations and supporting functions. This group will need to (1) establish a baseline of the resiliency of current State government operations; (2) establish a process to regularly assess cybersecurity infrastructure and activities within all executive branch agencies; and (3) identify cybersecurity awareness training needs for state employees.

Group Lead: Scott DePasquale, Chief Executive Officer, Utilidata, Inc. (Commission Chair)
Members: Peter Gaynor, Director, Rhode Island Emergency Management Agency
Thom Guertin, Chief Digital Officer, Rhode Island Office of Digital Excellence
B.Gen. Jim Jaeger (USAF ret.), Chief Cyber Services Strategist, Fidelis Cybersecurity
Ray Musser, VP Global Security Operations (retired), General Dynamics
Colonel James Vartanian, Director, Plans, Operations & Training, R.I. National Guard

2. Rhode Island National Guard Development Working Group

The Rhode Island National Guard has substantial capabilities related to detecting, analyzing, and researching network intrusions and vulnerabilities, primarily through the 102nd Network Warfare Squadron (NWS). The 102nd NWS houses a significant number of citizen airmen that currently engage with the RI Cyber Disruption Team. However, DoD policy and legislative barriers constrain their ability to fully integrate with State government and the private sector—limiting their role in normal operating conditions to assistance in training and advice. This group should assess: (1) what broader role the RI National Guard (RING) could play in helping to secure both State government and the private sector in RI; (2) what policy and legislative actions would be required to de-constrain the RING's role; (3) what opportunities exist to broaden the mission of the 102nd NWS related to the DoD, USAF, and US Cyber Command—with a focus on developing a platform that would merit longer-term increases in force structure; (4) what opportunities might exist for closer collaboration and training with NSA and US Cyber Command at Fort Meade; (5) what role could the RING play if a larger integration and sharing hub were established in RI; and (6) what funding opportunities exist within the RING to support further development of cybersecurity infrastructure in Rhode Island.

Group Lead: Colonel James Vartanian, Director, Plans, Operations & Training, R.I. National Guard
Members: R. Adm. Michael Brown (USN Ret.), VP Public Security, RSA
Scott DePasquale, Chief Executive Officer, Utilidata, Inc. (Commission Chair)
Vladimir Ibarra, Deputy Director, Providence Emergency Management Agency
B.Gen. Jim Jaeger (USAF ret.), Chief Cyber Services Strategist, Fidelis Cybersecurity
Macky McCleary, Director, Rhode Island Department of Business Regulation
Derek Reveron, Professor of National Security Affairs, U.S. Naval War College

3. State Police and Forensic Development Working Group

The Rhode Island State Police currently plays a critical role in supporting the RI Cyber Disruption Team, managing the State Fusion Center, policing state-wide cyber-crimes through the Computer Crimes Unit (CCU), and managing the Computer Forensics Laboratory. The CCU has substantial capabilities related to the collection, preservation, and analysis of computers and digital evidence, as well as providing forensic response at crime scenes and large computer incidents. This working group should consider what opportunities exist to further build on these forensic capabilities and what expanded role the State Police might play in providing expert assistance to other requesting statewide and federal law enforcement agencies, with investigations pertaining to the criminal use of computers and related technologies. Some focus should be given to what opportunities exist for closer collaboration with the various federal agencies engaged in cyber-forensics. Related to the deliverables for the October report, the working groups should also: (1) identify gaps and opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information; and (2) develop a framework for coordinated responses, simulation testing, and mutual assistance by executive branch agencies and the private sector to cyber incidents.

Group Lead: Colonel Steven O'Donnell, Superintendent, Rhode Island State Police
Members: Stephanie Douglas, Senior Director of Corporate Security, Pacific Gas & Electric
Peter Gaynor, Director, Rhode Island Emergency Management Agency
B.Gen. Jim Jaeger (USAF ret.), Chief Cyber Services Strategist, Fidelis Cybersecurity
Mark Levett, Chief of Strategic Partnerships Unit, Counterintelligence Division, FBI HQ
Doug White, Director of Applied Networking and Security, Roger Williams University
Victor Fay-Wolfe, Director of Digital Forensics, University of Rhode Island

Working Groups Related to Workforce and Industry
Steps the State should take to support the growth of a cybersecurity industry and workforce

4. Information Sharing and Integration Center Development Working Group

Cyber information sharing and integration centers can provide a vital linkage between government, the private sector, and academia. Several models have emerged, and best-practices continue to evolve around the role state government plays in driving the development of these centers regionally. There may be an opportunity in Rhode Island to stand up a larger integration hub/center-of-excellence, though the value proposition across the various stakeholders needs to be further assessed. This working group should consider whether or not a more aggressive approach to standing up a larger CoE is warranted, and what functions it would serve (i.e., research and development, information sharing, training and workforce development, etc.). Also, towards the goals of the December report deliverable, the group should: (1) take inventory of existing businesses in the cybersecurity industry within the State; (2) survey public and private institutions of higher education on cybersecurity related research and development activities; and (3) determine barriers to expand workforce and business development opportunities and provide recommendations on eliminating those barriers.

Group Lead: R. Adm. Michael Brown (USN Ret.), VP Public Security, RSA
Members: Gil Bishop, Chief Information Security Officer, Amica Mutual Insurance Company

Teresa Durocher, Director, Information Security & Technology Risk, Fidelity Investments
Suma Gaddam, Chief Information Officer, Care New England
Mark Munkacsy, Senior Engineering Fellow, Raytheon Integrated Defense Systems
Derek Reveron, Professor of National Security Affairs, U.S. Naval War College
Graham Wright, Chief Information Security Officer, National Grid

5. Workforce Development and Skills Training

A 2010 cybersecurity workforce development report from Carnegie Mellon University notes that organizations are faced with the challenge of ensuring that their workforce possesses the most current knowledge, skills, and experiences related to cybersecurity, with an emphasis on proficiency and relevance. The report further notes that "this issue is particularly challenging for a cybersecurity workforce because industry trends, practices, and technologies are constantly changing". Training and skills development related to cybersecurity are critical components to supporting even the most basic industries, let alone the development of a robust cyber-industry. It is critical to understand how programs are developed and financed through both academia and the private sector. This working group will: (1) conduct an assessment of the current cybersecurity workforce development and education activities in the State, including curricula, certificates, and training credits offered; and (2) develop a set of recommendations to address both gaps and opportunities.

Group Lead: Molly Magee, Executive Director, Senedia
Members: Matt Cullina, Chief Executive Officer, IDT911
Chuck LoCurto, Chief Information Officer, Bryant University
Macky McCleary, Director, Rhode Island Department of Business Regulation
Stefan Pryor, Secretary, State of Rhode Island Executive Office of Commerce
John Savage, Professor of Computer Science, Brown University
Francesca Spidalieri, Senior Fellow for Cyber Leadership, Salve Regina UniversitY
David Wilga, Vice President & Chief Technology Officer, RI Airport Corporation

VIII. ANNEX 2—REFERENCES

[i] Price Waterhouse Coopers "Global State of Information Security", September 30, 2014.

[ii] Lloyd's, Emerging Risk Report – 2015 "Business Blackout", July 2015.

[iii] Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Committee, January, 2014

[iv] National Cybersecurity Center of Excellence (NCCoE), "Center," http://nccoe.nist.gov/content/center.

[v] Commission on Maryland Cybersecurity Innovation and Excellence, "Final Report: Findings and Recommendations," September 1, 2014, p. 10.

[vi] Maryland Department of Business and Economic Development, "Cybersecurity Investment Incentive Tax Credit," http://business.maryland.gov/fund/programs-for-businesses/cyber-tax-credit.

[vii] Texas Department of Information Resources, "The Archer GRC Portal," http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=136.

[viii] NASCIO & California Department of Technology, "NASCIO 2014 State IT Recognition Awards: California Cybersecurity Task Force," May 2013, p. 2.

[ix] "NASCIO 2014 State IT Recognition Awards: California Cybersecurity Task Force," p. 3.

[x] California Office of the Governor Edmund G. Brown, "Governor Brown Signs Executive Order to Bolster Cybersecurity," August 31, 2015, http://gov.ca.gov/news.php?id=19082.

[xi] Office of the Governor, "McAuliffe Names Members of Virginia Cyber Security Commission," Press Release, May 16, 2014, https://governor.virginia.gov/newsroom/newsarticle?articleId=4817.

[xii] Virginia Cyber Security Partnership, https://cyberva.virginia.gov/media/3637/va-cyber-security-commission.pdf.

[xiii] Virginia Government, "Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats," *Press Release*, April 20, 2015, https://governor.virginia.gov/newsroom/newsarticle?articleId=8210

[xiv] Virginia Government, "Governor McAuliffe Signs Executive Order to Strengthen Cybersecurity Protocol," *Press Release*, August 31, 2015, https://governor.virginia.gov/newsroom/newsarticle?articleId=12544.

[xv] "Idaho governor creates task force to battle hackers," Betsy Z. Russell, August 2, 2015. http://www.idahostatesman.com/2015/08/02/3921429/idaho-governor-creates-task-force.html

[xvi] Idaho governor establishes cybersecurity task force," Grayson Ullman, July 30, 2015. http://statescoop.com/idaho-governor-establishes-cybersecurity-task-force/

[xvii] Eric Anderson, "National Guard to Provide Cybersecurity," *Times Union*, November 17, 2014, http://www.timesunion.com/business/article/National-Guard-to-provide-cybersecurity-5899638.php.

[xviii] Office of the Governor, "Defending New Jersey's Digital Density: Governor Christie Signs Executive Order Establishing the NJ Cybersecurity and Communications Integration Cell," Press Release, May 20, 2015, http://nj.gov/governor//news/news/552015/pdf/20150520b.pdf