PREPAREDNESS LEADERSHIP COUNCIL

INTERNATIONAL

A changing global threat environment, coupled with increasingly interdependent societies and aging infrastructures, is a dangerous combination that must be addressed by today's preparedness leaders.

May 2016

Cybersecurity
A Way Forward

Thomas Lockwood

Foreword by Thad William Allen

Published by the IMR Group Inc.
Distributed by DomesticPreparedness.com
Severna Park, Maryland

Cybersecurity
A Way Forward

By Thomas Lockwood

Foreword by Thad William Allen

The Preparedness Leadership Council International

The Preparedness Leadership Council International (PLC), formerly the DomPrep40, is a thought leadership group comprising insider practitioners and opinion leaders who offer advice and recommendations on topics relevant to emergency planners, responders, receivers, local-state-federal authorities, nongovernmental organizations, and the private sector. Focusing primarily on prevention, protection, response, recovery, and mitigation, the PLC is tasked with developing quantifiable and quantitative feedback from surveys and roundtable discussions that is gathered from and shared with a broad multidiscipline, multi-jurisdictional audience of operational professionals and policy advisors. Information shared via the publications: DomesticPreparedness.com (online and mobile), *DP Weekly Brief* (email newsletter), and the *DomPrep Journal* (PDF download).

DomesticPreparedness

DomPrep is an information service for the preparedness and resilience community. Created in 1998, offers content–provided by practitioners and subject matter experts–to tens of thousands of first responders, medical receivers, emergency planners, local-state-federal authorities, nongovernment organizations, and private-sector professionals.

Note: all comments provided in this report reflect the opinions of the individuals and do not necessarily represent the views of their agencies, departments, companies, or organizations. Quotes within the report without acknowledgment were made anonymously by respondents.

IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900;
email: subscriber@domprep.com; also available at www.DomesticPreparedness.com

ABOUT THE AUTHOR

Thomas J. Lockwood is a trusted advisor to senior level officials within federal and state governments and the private sector, providing guidance in areas such as crisis management, policy and program development, best practices, and strategic execution. He is a former member of Department of Homeland Security's (DHS) senior leadership team and served its secretaries in key leadership roles. As chair of the Inter-Agency Credentialing Committee, he directly influenced the creation of national policy and architecture for high-assurance identity and piloted multiple physical and logical use cases. He supported the White House cybersecurity coordinator in efforts to secure online transactions as lead coordinator and core team member for enhancing security and privacy. He is an active participant in multiple federal and commercial standards and publications efforts, interagency and intergovernmental collaboration efforts, and public-private trust framework engagements. He served as the DHS director for the National Capital Region, the homeland security advisor and deputy director of homeland security for the State of Maryland, and the executive deputy commissioner for Homeland Security & Emergencies for the State of New York. He also served as leader and team member of design build teams, which included major defense systems, industrial facilities and processes, safety and reliability systems, systems integration, and net-centric systems. He is currently an elected board member of the Smart Card Alliance and member of the board's Leadership Committee, representing over 200 members worldwide. He is a board representative to Committee on Councils & Chapters, IoT Security Council, and Identity Council. He is an advisory committee member to the *DomPrep Journal* and a member of the Preparedness Leadership Council International. He is a former Brookings Institution fellow, a graduate of the Harvard Business School and chairman of his Class, and past president of the Navy's Association of Scientists and Engineers.

–This page was left blank intentionally–

TABLE OF CONTENTS

–This page was left blank intentionally–

ACKNOWLEDGMENTS

Cybersecurity is one of the greatest new challenges to public and private safety, security, and resilience. The world is in the early stages of understanding what it is, how to know when information and/or infrastructure has been breached, what the cyber linkages to physical systems are, and how vulnerabilities and consequences within a system-of-systems can be reduced. This threat is so hard to understand because it can be direct, indirect, veiled, conditional, or any combination thereof. Cyberattacks can be initiated by state-sponsored, rogue, criminal, recreational, domestic, or offshore actors. Identifying, responding to, and recovering from an attack or breach are moving beyond any single organization's capabilities.

Professionals in preparedness and resilience are looking for answers. Although this report will not answer every question, it will show how the greater Pacific Northwest Economic Region has developed, implemented, and refined leading approaches to cybersecurity preparedness and response. Through collaboration, leadership, and risk management, this region has developed a bottom-up solution. Although there is much work to be done, this report provides clear tangible steps and direction to strengthen regions by leveraging the strengths and capabilities of the public and private sectors. Hopefully, this report will serve as a benchmark to foster collaboration and partnership with other regions for consideration and adoption in their own regional efforts.

The Preparedness Leadership Council International (PLC) was privileged to host a working group roundtable in Seattle, Washington, to learn about the region's solutions and develop actionable items. This report was generated from that conversation, integrated with input from over 300 DomPrep survey participants, and presents key findings. Only through the support and patience of the Seattle-based working group's lead Michael K. Hamilton, plus David R. Matthews, Matthew Modarelli, Steven L. Stein, and Colonel Gent Welsh, is this report possible. Also, without the urging of PLC Executive Committee member, Vayl Oxford, we would not have gone to Seattle to learn about its vigilance. Thank you all.

My deepest appreciation goes to Timothy J. Lowenberg, major general (Ret.), vice president of Gordon Thomas Honeywell LLP and former Washington state adjutant general. General Lowenberg was a masterful moderator of the roundtable. We were also fortunate to have Thad Allen, executive vice president of Booz Allen Hamilton, the 23rd commandant of the U.S. Coast Guard, and national incident commander for the unified response to the Deepwater Horizon oil spill in the Gulf of Mexico, offer his expertise as a participant.

My humble apologies for this report being published late. My sincere gratitude goes to Thomas Lockwood, who recreated the event and rewrote the proceedings in order to present the findings and conclusions therein. Thank you, Tom.

Lastly, thank you to Booz Allen Hamilton, BioFire Defense, Emergent BioSolutions, and FLIR Systems. Without their financial support, this report would not have been possible. Finally, thank you to the DomPrep team including Catherine Feinman and Carole Parker. A good job by all, indeed.

Martin D. Masiuk
Executive Director
Preparedness Leadership Council International

–This page was left blank intentionally–

FOREWORD

We live in a connected society. The convergence of the internet and modern mobile devices is creating a revolution that touches every person, crosses boundaries, and simultaneously involves public, private, and nongovernmental organizations. In April 2015, the Preparedness Leadership Council International (PLC) drew together a diverse group of representatives from the Pacific Northwest to discuss the regional challenges facing a connected society, consistent with presidential guidance that encouraged the creation of information sharing and analysis organizations (ISAOs). Regionally focused ISAOs that form naturally around communities of interests are critical to addressing local economic priorities, promoting unity of effort to address common threats, building trusted relationships in advance of an event, and bridging existing gaps in the current national critical infrastructure protection framework. The conversation and insights from that meeting can inform how to organize, collaborate, plan, and act with common purpose – in effect, a whole-of-community response.

Cyberthreats present unique challenges that do not neatly fall into existing policies, doctrine, and tactics related to emergency response. For that reason, it is important to discuss and test assumptions regarding incident management, communications, intergovernmental coordination, and cross-sector collaboration in advance. The results of the PLC discussion documented in this report affirm the value of ISAOs, but, beyond that, provide insight into strategies for shared services, the need to understand incident response in the context of the National Incident Management System, the value of including cyberthreats in planning and exercises, and the important synergy of partnerships.

The Pacific Northwest has a unique representation of academic institutions, aerospace technology, information technology, high-tech manufacturing, critical transportation infrastructure, military bases, and international maritime transportation waterway that is jointly managed by the United States and Canada. I was honored to have been a part of this effort, and to have engaged with this community of informed, dedicated leaders. The conclusions and recommendations contained in this report are a valuable resource for like-minded communities across the country that are looking to unify their planning and response capabilities. My thanks to PLC and to all who made this possible.

Thad William Allen
Preparedness and Response Professional
Admiral, U.S. Coast Guard, Retired

–This page was left blank intentionally–

SUMMARY

In an increasingly interconnected world of cyberthreats and defenses, the greater Pacific Northwest Economic Region – particularly Washington State and its Seattle area – has emerged as a national and international leader in information technology. This region has developed, implemented, and refined leading approaches to cybersecurity preparedness and response, collaboration, leadership, and risk management. The Preparedness Leadership Council International (PLC) roundtable discussion on cybersecurity was held in Seattle, Washington, on 27 April 2015, and sought to identify key accomplishments, continuing challenges, and potential solutions for cybersecurity collaboration. The discussion aimed not only to benefit the Pacific Northwest, but to develop exemplifying programs and patterns to share with other local, state, and national regions navigating the cyberworld's sprawling dangers and opportunities.

Thirty-six senior subject matter experts representing private sector and not-for-profit organizations, as well as local, state, and federal governments, attended the roundtable. The detailed discussion elicited five broad key issues affecting cybersecurity in the region. The key issues, described as follows, provide the framework for this report.

Key Issues

I. ***Regional Collaborative Traits.*** Effective cybersecurity is inherently dependent on public and private collaboration. As a regional "cluster" for everything information technology (IT), this area has become particularly adept at pooling knowledge and resources across these sectors. This successful collaboration is bred from talented executive leadership, strong regional relationships, and interpersonal trust. Key regional collaboration areas include infrastructure protection, workforce development, research strategies, and related policymaking. Of particular note are the region's strategic efforts to create shared service capabilities across the region, supporting wider preparedness and response planning for the community as a whole.

II. ***A Common Understanding.*** As an IT cluster, this region is an enhanced target for cyberattacks. As such, cybersecurity is commonly viewed as a matter of public safety and economic priority. Because of this uniquely strong common understanding in both the public and private sectors, critical infrastructure and key life-safety resources inherently hold high priority. In order for agencies to partner in planning and development efforts, however, they must have more than this shared view: mutual aid structures must be refined, and common language and credentialing

must be established. Trusted formal and informal support structures, including routine in-person exchanges at executive and operational levels, allow all stakeholders to commonly assess and mitigate risks.

III. ***Information-Sharing Structures and Mechanisms.*** In order to foster a common understanding, information must be shared across all regional sectors and disciplines. Trust is integral to this communication. In Washington State, not-for-profit and private organizations serve as "trusted third parties," bridging critical process, organization, and discipline gaps between the sectors. Effective information sharing must flow between all levels of participants, with contributors' efforts being recognized and reciprocated. To practice this two-way flow, the state's IT experts have developed formal public-private coalitions, forums, fusion centers, and academic partnerships. Critical sensitive data is vetted quickly through the public sector to reach the appropriate cyber response stakeholders in the private sector, allowing mitigation and response to occur in a timely manner.

IV. ***Planning and Preparedness.*** The region's collaborative successes have allowed area professionals to identify significant barriers to planning and preparedness. Incident command structure, roles and responsibilities, and practices to support cyber incidents are not well understood, documented, or routinely practiced. Mutual aid structures and mechanisms, common language, resource typing, and credentialing are especially critical for physical and logical access and response to cyber events. The public sector is working to introduce private sector IT professionals to National Incident Management System (NIMS) and Incident Command System (ICS) concepts. Additionally, the region is raising awareness of third-party product and service provider risks and interdependencies.

V. ***Policy Framework.*** All stakeholders at all levels – in both sectors – must work to clarify, prioritize, and establish a resolution framework. With a framework in place, they can begin to resolve legal and policy barriers to preparedness and response, develop agreement solutions, and follow through with policy decisions. Current Emergency Management Assistance Compact (EMAC) policy must be revised to facilitate the maximum use of all available resources within member states and the private sector. Technical and administrative policies are needed to strengthen awareness and actionable information sharing. A good policy framework would, for example, promote anonymity of information reporting and reputation scoring, and corroborate information.

With these key issues defined, the PLC created a nationwide survey for the *DomPrep Journal (DomPrep)* audience to provide additional input and comments. The information provided by the 337 *DomPrep* readers who responded to the survey has informed this report, and the results are found in figures throughout.

Recommendations

Exploring findings from the established key issues, this report offers specific recommendations for policymakers and stakeholders to overcome the identified cybersecurity shortfalls and challenges. These recommendations include:

- Revise EMAC to facilitate the maximum use of all available resources – within member states' public and private sectors – that are unique and necessary to support response to a major event.
- Support awareness and adoption of ICS/NIMS concepts within the cyber community. Comparable strategies for cybersecurity and response should be developed and reflected in cyber annexes to response plans.
- Develop and sustain effective partnerships between public and private organizations. In doing so, allow not-for-profit and other private entities to serve as trusted third parties that bridge cross-sector and cross-discipline processes and mechanisms. Partnerships should promote regional relationships, information sharing, and coordination of processes (for example, Pacific Northwest Economic Region (PNWER), Cyber Incident Response Coalition and Analysis Sharing (CIRCAS).
- Include IT system availabilities, dependencies, and interdependencies and cyber impacts in exercise planning and development as a matter of course. Exercises should consider system failure points, third-party product and service providers, and continuity of operations (including viability of telework and remote access from an external environment impacted by a cyber event).
- Develop and document a common public and private understanding of critical resources. Resources should clarify common language, resource typing, awareness, access and sharing, and legal agreements before an event.
- Develop common policy for authentication of credentials, attributes, and claims for physical and logical operations. The policy should support interoperability and multi-factor digital authentication to confirm that individuals are who they claim to be and they possess the competencies, skills, certifications, and permissions they claim to possess.

- Refine and support information-sharing mechanisms across executive and operational levels. Mechanisms should take into account various levels of risk and have capabilities for support monitoring, detection, sharing of sensitive and secure information, and sharing of response information (for example,, Public Infrastructure Security Collaboration and Exchange System (PISCES), Regional Economic Cyber Analytics Platform (RECAP), Distributed Incident Management System (DIMS).

- Promote definition and adoption of common contract language or requirements addressing security and integrity of third-party product and service providers.

- Support and further enhance cyber shared-service and managed-service strategies. These strategies provide access and affordability of cyber competency and capabilities to traditionally under-resourced entities. They also address traditional vulnerabilities and strengthen federated resilience and operations.

This report is meant to lay the groundwork for key leaders' and policymakers' careful consideration. The information provided herein is generally reflective of the opinions voiced at the PLC meeting (and by the survey respondents). However, any given statement should not necessarily be viewed as consensus.

Cybersecurity roundtable discussion, Seattle, WA.

INTRODUCTION:
INFORMATION-SHARING ORGANIZATIONS IN CONTEXT

"We need to start talking about cybersecurity and threats."
– Peter Gruen, RN, Erie County Department of Health and Emergency Preparedness

Information technologies have transformed society. Cyber connectedness has integrated the economy, public and private sector operations, and our private lives. It has revolutionized how people communicate – whether with a friend down the street or a colleague across the globe. This transformation has bloomed into in an "Internet of things" – the connected digital networking and interaction between products, systems, and people. The rapid and vastly positive changes that have followed the rise of information technology have, however, challenged security. As the nation becomes increasingly vulnerable to potentially life-threatening cyber-attacks, preparedness and response efforts cannot be compartmentalized. Communication and readiness activities must be as interconnected as the systems that are under attack.

The State of the Nation

America already possesses strong formal and informal information-sharing mechanisms across the public and private sectors. Public-private partnerships, not-for-profit and non-governmental organizations (NGOs), informal and private groups, and public agency lead groups exist to bridge knowledge gaps in critically related fields. But in the increasingly precarious area of cybersecurity, the nation's organizations have yet to fully come together to prevent and prepare for potentially devastating threats.

On the national level, public-private partnerships and NGOs are the principle mechanisms supporting public and private sector cyber collaboration. InfraGard, for example, created in 1996, is a public-private partnership that links U.S. businesses with the FBI to foster cooperation, preparedness, and response within the private sector. Building on these efforts, in 1998, the federal government fostered the creation of information-sharing and analysis centers (ISACs) to coordinate various critical infrastructure sectors. State, local, and tribal governments have historically supported similar participation in NGOs and not-for-profit organizations – including groups inclusive of small businesses, medium businesses, and subject matter experts. This traditional local strategy in harmony with the expanding federal strategy provides potential for scalability and focus, with a foreseeable outcome of richer information sharing and exchanges.

In February 2015, President Obama issued Executive Order 13691, entitled *Promoting Private Sector Cybersecurity Information Sharing*. The order's intent was to encourage cybersecurity threat information sharing within the private sector, and between the

private sector and the government. To do so successfully, the order calls for regions to establish information-sharing and analysis organizations (ISAOs).[1] Intended to address ISACs' weaknesses, ISAOs represent a more inclusive and flexible approach to self-organized information-sharing activities, aligned with the needs of all stakeholder groups. ISAOs may be existing or may be organized on any number of bases, such as in response to specific emerging cybersecurity threats. ISAOs span across both public and private sectors, and can be formed as for-profit or not-for-profit entities. The Department of Homeland Security further explains that ISAOs should be:

- ***Inclusive*** – They should include groups from any and all sectors, not-for-profit and for-profit organizations, and both experts and novices.
- ***Actionable*** – They should be enabled to receive, provide, and exchange information about useful and practical risk, threat indicators, and incident information via automated, real-time mechanisms.
- ***Transparent*** – They should share a common understanding about how the model operates and meets their needs.
- ***Trusted*** – They should have the ability to receive and share sensitive information, including information shielded from release – as otherwise required by the Freedom of Information Act or state sunshine laws – and should be exempt from regulatory use and civil litigation.

To foster cohesiveness, the President's order empowers an NGO to serve as the ISAO Standards Organization. This organization is tasked "to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs."[2] Through public, open-ended engagements, the ISAO Standards Organization will develop transparent best-practices operations that align with the order's intent. The Standard Organization's guidelines should outline baseline capabilities and requirements – including contractual and operations-related arrangements – and privacy protections – such as minimization and information-sharing methods that protect privacy and civil liberties.

A Regional Path to Follow

Based on its accomplishments, the greater Pacific Northwest Economic Region – particularly Washington State and its Seattle area – appears not only to align with the President's envisioned model, but to exemplify it. A leader in information technology, cybersecurity, collaboration, and homeland security, the region possesses not only a wealth of public-private partnerships, NGOs, and private groups, but has also pioneered informal cybersecurity information sharing. Through the leveraged combination of federal-sponsored and grassroots local models, the region has developed leading approaches to

cyber preparedness, response, and recovery. These regional leaders and their efforts set an operational example for other regions and ISAOs to emulate, and could potentially serve the nation as a benchmark for the ISAO Standards Organization.

On 27 April 2015, the Preparedness Leadership Council International (PLC) hosted a roundtable discussion in Seattle for national subject matter experts and regional public and private sector information security leaders. In order to document the region's dynamics, accomplishments, challenges, and ongoing activities, discussion was approached by way of four core topical areas: (1) Understanding ISAOs: What are ISAOs? How are they best founded, organized, and funded? Do they present an improved alternative to information-sharing and analysis centers (ISACs)?; (2) Identifying original incidents: What do left-of-boom, center-of-boom, and right-of-boom scenarios look like? What are the advantages and disadvantages of organizing "cyber mutual aid" agreements?; (3) Defining the role of dedicated in-house cyber crisis managers: Should these managers be under contract or obtained through cyber insurance?; and (4) Managing incidents: What role do the National Incident Management System (NIMS) and Incident Command System (ICS) play in cybersecurity?

The discussion elicited five broad key issues affecting cybersecurity in the region. The key issues, described as follows, provide the framework for this report:

- Regional collaborative traits
- A common understanding
- Information-sharing structures and mechanisms
- Planning and preparedness
- Policy framework issues

The experts agreed that the policies, processes, technology, enforcement, and governance methods being created in Washington State could–and should–be developed, documented, standardized, and disseminated to other areas around the country, and even possibly shared with international partners.

Although this report reflects the sentiments of the many experts who participated in the discussion, it is not an exhaustive analysis of their recommendations or a completely realized roadmap for implementing those recommendations. It is meant to lay the groundwork for the next step: key leaders' and policymakers' careful consideration of the recommendations. The information provided herein is generally reflective of the opinions voiced at the meeting (and by the survey respondents); however, any given statement should not necessarily be viewed as consensus.

I. UNIQUE REGIONAL COLLABORATIVE TRAITS

Today's economic world map is dominated by *clusters:* critical masses, in one place, of unusual competitive success in particular fields.[3] Clusters are a striking feature of virtually every national, regional, state, and even metropolitan economy, especially in more economically advanced nations. Clusters have the potential to affect competition in three ways: by increasing the productivity of the companies in the cluster; by driving innovation in the field; and by stimulating new businesses in the field. The U.S. Council on Competitiveness identifies the Greater Seattle-Bellevue-Everette area as one such cluster for advanced information technology and applications.

Excelling in information technology, this region has particularly adept resources for product and service integrity. Both public and private sector leadership prioritize their contributions to IT and cybersecurity. This leads to a common understanding, alignment and support of strategic policies, and unity of leadership vision and direction. Regional executives and thought leaders actively support, participate in, and trust not-for-profit organizations and public-private partnerships that promote regional cyber focus, capabilities, and relationships.

The region's IT cluster further attracts talented cybersecurity professionals who are looking to practice in an energized environment. With an engaged workforce, the cluster develops and matures a greater concentration of leadership and workers across both public and private sectors. Individuals in this field, in this region, are lauded for strong information technology and cybersecurity competence – including design-build and operational experience – and inclusiveness of information technology and cybersecurity risk mitigation within products and services.

As this cluster thrives, it fosters an environment of collaboration. It breaks down instructional "laterals" or cross-sector barriers to sharing, and enhances daily operations that directly contribute to unique collaborative efforts. Some of the region's most notable collaborative achievements include:

- Developing a strategic leveraging strategy between the public sector, private sector, and academic community to mutually support: (a) infrastructure protection; (b) workforce development; and (c) research strategies, policies, and related activities.

- Exposing information technology and cyber professionals to ICS/NMS concepts and strategies, and supporting development of comparable strategies for cybersecurity.

- Integrating cyber policies and issues within exercises and planning activities.
- Developing and supporting shared service strategies to provide cyber competency and capabilities, including support to traditionally under-resourced local jurisdictions.

II. GAINING A COMMON UNDERSTANDING

"As a society, our quality of life is dependent on our cyber systems, and they in turn are dependent on our public infrastructure. Awareness is the beginning step to create the much-needed public-private cooperation."

– John Morton, Senior Advisor, *DomPrep Journal*

The rise of information technology has led to rapid – and vastly positive – changes, but has also posed significant new challenges and vulnerabilities. Cybercrime costs the global economy over an estimated $400 billion per year. In 2013, in the United States alone, approximately 3,000 companies' systems were criminally compromised.[4] Regardless of impetus – whether for money, ideology, conscience, or ego – individuals, organizations, state-sponsored activities, and nation-states are actively seeking to undermine or control the very capabilities that have transformed society. Public and private sector leaders now place cyber risk firmly at the top of their agendas. High-profile breaches raise fears that hack attacks and other security failures will increasingly endanger the economy and security.

In Washington State, cybersecurity is a pervasively recognized direct threat. As a leader in the global aerospace, communication, and IT sectors – as well as in advanced manufacturing, life sciences, and defense – Washington State is disproportionately attractive to threat actors. Cybersecurity in this area is viewed not only as a matter of public safety, but also as an economic issue. Beyond its intellectual and proprietary property contributions to the region, Washington is also the fourth-largest exporting state in the United States. With its ports handling 8 percent of all American exports and receiving nearly 6 percent of the nation's imports, over US$500 billion in goods pass through the state's shores annually.[5] As such, cybersecurity is a shared executive priority in both the public and private sectors.

The region has gained a common understanding of several points that underpin this shared ideology. In general, these include:

- Regional cyberstrategies rest on building and renewing strong interpersonal relationships, and bringing the right public and private sector people to the table to share information and resources.

- Communication is integral to establishing a common operating picture. Trusted formal and informal support structures at the executive and operational levels – including routine in-person exchanges – are enhanced by the ability to electronically share information and analysis at various levels of risk and access.

- Information sharing must occur and flow between *all levels of participants* – from federal, state, tribal, and local governments as well as the private sector – with contributors' efforts being reciprocated.

- Critical infrastructure and key resources have the most serious vulnerabilities (especially regarding local life-safety systems like 911, dispatch, and radio) and are therefore given higher priority than commercial sectors and businesses.

- Participants need to be aware of third-party dependencies and vulnerabilities, and a false sense of security through third-party vendors and service providers.

III. INFORMATION-SHARING STRUCTURES AND MECHANISMS

"[Cybersecurity] is not just an IT issue. It is everyone's issue. We all have a role to play."

– Robert Fink, Emergency Management Specialist, Bucks County, PA

Without foundations of trust, information sharing is not possible. In Washington State, dozens of organizations have developed trusting relationships and information-sharing structures that support cybersecurity preparedness and response. These relationships include not-for-profit and NGOs, public-private partnerships, formal and informal private groups, and public-agency lead groups. Once established, the personal and professional relationships reinforce regional cohesion against a common threat.

In order for this region's many information-sharing mechanisms to work, the common goal takes precedence over traditional industry competition. Rather than competing for information, organizations come together through channels of choice based on community/sector demographics and individual needs. Choice empowers organizations, buyers, and users alike to determine how information is shared, and how each stakeholder can participate and exchange content.

Through collaboration, strong leadership, and daily operations and interactions, the region has conceived, defined, and adopted, information-sharing structures and mechanisms that it continues to enhance. These can be generally characterized as:

(a) information-sharing *organizations,* which have exchanges and capabilities supporting the executive, direct-management levels; (b) *systems* that support operations, which include response systems, as well as systems that monitor and detect sensitive or secure information at multiple classification levels; and (c) *shared services*, which include analytics, coordination, and common capabilities.

Combined, these mechanisms' benefits range from dissemination of need-to-know information, to real-time analysis and assistance, to preparation for regional events that may exhaust individual organizations' response capabilities. These key information-sharing structures and mechanisms serve as benchmarks for other regions and should be leveraged when designing a model ISAO with an integrated focus on regional priorities. A detailed discussion of each mechanism structure is provided in the following sections.

Regional Information-Sharing Organizations

Not-for-profit and public-private partnerships take a leading role in executive and managerial-level information sharing. Of particular importance, these partnerships effectively serve as trusted third parties. With the power to convene, the third parties are capable of leveraging information and communicating about processes to bridge cross-sector, cross-discipline gaps. This helps break down information silos and integrate communities of interest in the cyberthreat profile. The organizations that participate in these exchanges comprise existing councils, committees, and other bodies that have regional authority and inherent accountability. Key among them include:

- ***Agora*** – Agora may be considered the original ingredient from which Washington State's cybersecurity "secret sauce" was blended. Founded almost 20 years ago by a small group of chief information security officers in the Puget Sound region, its quarterly meeting brings together an ever-increasing trusted community of senior-level information security practitioners. Each meeting is an opportunity to share new intelligence, meet other information security personnel, learn about new initiatives and available positions, and hear presentations from some of the leading experts in the field. Over 300 participants regularly attend, some traveling from the East Coast or from Canada and other international locations.

- ***CIRCAS*** – Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) is an information-sharing forum. Its innovative process brings industry professionals together to discuss threat intelligence, information security best practices, and resources (such as expertise, hardware/software, and personnel). CIRCAS was originally formed as a strategic response to a national cyber exercise that took place in the Puget Sound area – the Emerald Down 2013 Exercise. The exercise determined that regional emergency operations,

as defined by NIMS and the Emergency Management Assistance Compact (EMAC), did not provide adequate structures for mutual aid in response to major cyber disruption events. Preparedness resources typically leveraged for other types of emergencies were not being leveraged for cyber emergencies. Specific deficiencies included acquisition of professional resources and equipment, and unique NIMS resource typing, credentialing, and indemnification requirements. CIRCAS now brings community professionals together to prepare for cyberthreats the way they prepare for other emergency or disaster situations. In the event of a cyberattack that results in regional disruption of infrastructure, CIRCAS members serve as volunteer responders. Their inclusion is anchored in the Washington State emergency response plan's cybersecurity annex.[6]

- ***PNWER*** – Pacific Northwest Economic Region (PNWER) is a collaborative regional organization dedicated to addressing common issues and interests, such as encouraging global economic competitiveness and preserving the natural environment. It is designed to improve cooperation and communication between member jurisdictions as well as to improve communication between the public and private sectors. PNWER provides the sectors with a cross-border forum for unfiltered dialogue. The organization capitalizes on the synergies between business leaders and elected officials who work to advance the region's global competitiveness.

Regional Information Systems

Trust in interpersonal and inter-organizational relationships alone – though it is an integral component – cannot fully engender preparedness. Regional leaders must also be able to trust the technical systems that allow monitoring, detection, analysis, and sharing of time-sensitive information and capabilities across the region. Regional information systems support dynamic, immediate, and somewhat automated information sharing to stakeholders. In the Washington State approach, this function is filled by two regional monitoring systems, which are overseen by a fusion center's embedded analyst. This system features a shared information service that monitors security events occurring on public networks in order to provide detection, alert, and response services, as well as an understanding of cyberthreats and cyberattacks targeting the region. Along with detecting compromised assets and isolating compromised sites, the regional monitoring provides assistance to academic programs, including workforce development and continuing system research.

- ***PISCES*** – The Public Information Security Communication and Exchange System (originally known as Public Regional Information Security Event Management, or PRISEM) is a shared regional cybersecurity monitoring system. PISCES aggregates and processes cyber event data, provides correlated alerts on threat conditions, and extends situational awareness for public sector organizations across the Puget Sound area. Currently, PISCES serves seven cities and counties, six maritime ports, one hospital, two energy utilities, and the SeaTac airport, with expansion underway. Integrated with analysts at the Washington State Fusion Center, PISCES is the only such system in the United States.

Information is contributed to PISCES by participating organizations through the use of collectors – firewall logs, netflow, server logs, Intrusion Detection System (IDS) alerts, etc. The results are aggregated and then correlated within the organization and across the region, and alerts are presented to an analyst in the Washington State Fusion Center. The analyst receives indicators of compromise from the federal government, ISACs, and other sources, and searches the region for those indicators. When compromised Internet sites are found to be causing the source of compromised assets in the region, the analyst works with those sites to have them repaired. More than just distributing another "block list," this activity actually makes the internet a safer place. This approach is an operational example of the National Governors Association recommendation to leverage fusion centers' capabilities with embedded cyber analysts to assist a state or region. Demand for PISCES capabilities is driving the evolution and establishment of a larger multistate initiative, the Regional Economic Cyber Analytics Platform (RECAP).

- ***DIMS*** – The Distributed Incident Management System, developed by the University of Washington, is an online, anonymous, trusted information exchange tool. DIMS provides PISCES/RECAP member organizations a required tool for private communications during an incident (whether regional or confined to a single organization) and for sharing capabilities and information. DIMS is also designed to ingest data from regional monitoring and is the de facto interface for investigation and analysis by regional information-sharing and analysis organizations. A pilot project is underway in which trusted organizations/personnel are strictly vetted and authorized to access the system. Similar to PISCES (and using the same collection mechanisms an addition to newer, more robust versions), DIMS will collect data flow information, correlate it with threat intelligence feeds from an extensive variety of resources, and disseminate alerts and threat information to participants.

Regional Shared Services and Leveraged Strategies

The region has developed several innovative common services that support enhanced regional preparedness and response, access to key competencies and capabilities, and address key shortfalls between the traditional "haves" and "have-nots" in the industry.

- ***The National Guard and Emergency Management Division*** – The Washington National Guard and the state's Emergency Management Division were early and strong supporters of cyber preparedness and response initiatives. Through facilitating integrated project teams, performing assessments of infrastructure, and serving as the liaison to the Department of Homeland Security, state military has been invaluable to the process of integrating once-disparate initiatives into a coordinated structure that is focused on infrastructure protection, workforce development, and research. The Guard has created teams comprising some of the best experts in cybersecurity, penetration testing, and malware analysis. With the help of these teams, the organization has been able to assist local utilities with cyber risk assessments and strategic planning. The Guard has also filled a coordination role in facilitating integrated project teams (IPTs) to move toward desired outcomes. These IPTs have produced an annex to the state's emergency management plan that is focused on managing a significant disruption event due to cyber means. To exercise the plan, the IPTs are working with the CIRCAS public-private partnership and others to identify opportunities for improvement.

- ***Washington State Fusion Center*** – The Washington State Fusion Center (WSFC) provides a critical regional service: supporting the public safety and homeland security missions of federal, state, local, and tribal agencies and private sector entities. In doing so, WSFC serves as the state's single fusion center for detecting, deterring, and preventing terrorist attacks and criminal activities. The center also performs threat assessment and information management services, including the protection of critical infrastructure and key resources. Law enforcement officers and professional intelligence analysts provide the experience and expertise necessary to drive the WSFC's operational model of "intake, analyze, and disseminate."[7] In its daily operations, the WSFC accesses classified intelligence that applies to the region and the expertise, and initiates means to take action on that intelligence. This includes hosting and empowering regional information-sharing systems and cyber analytical capabilities. This shared service is greatly enhanced by the capabilities and diverse experience of the embedded cyber analyst.

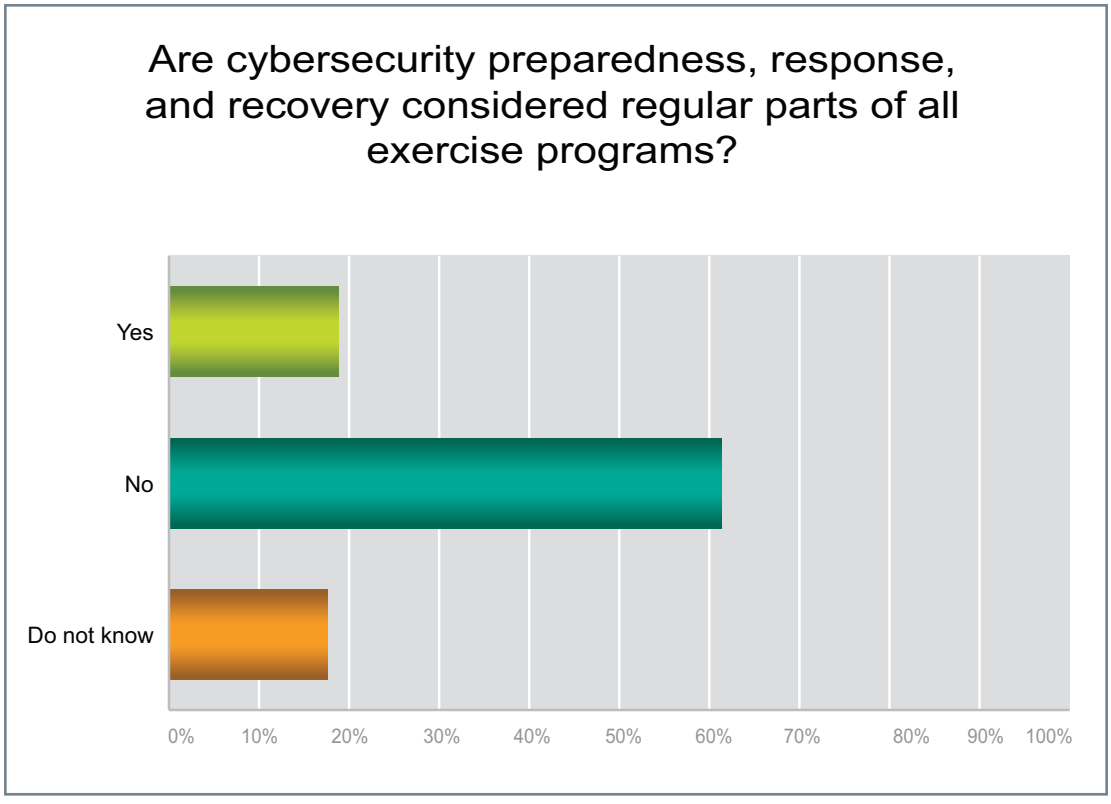
- ***Shared Analytical Capabilities*** – The WSFC provides another element that has enough value to stand as its own structure: a dedicated cyber analyst with cross-sector capabilities. Integrated with regional monitoring, the fusion center analyst serves as the "information-sharing broker," capable of informing the federal government through the existing Department of Homeland Security framework, but also of utilizing access to classified information to provide context or investigative assistance to the private sector. Over the last two years, the WSFC analyst has "touched" all but three U.S. states, coordinated findings with the wider fusion center network, and identified and stopped campaigns against regional law enforcement and financial officers, all while leveraging the existing investment made by state and federal governments in the fusion center.
- ***Collaborative Leveraging Strategy*** – A persistent problem for public infrastructure operators is the lack of qualified, affordable practitioners. In response, public and private sectors are partnering with the academic community to mutually support an innovative approach that leverages workforce development, infrastructure protection needs, and research activities. In a partnership with the state's academic institutions, these unique, benchmark-worthy programs include:
    - *CREATES* – A veteran reemployment program, CREATES brings together academics and private sector practitioners for a real-world experience and professional credentialing. In this program, veterans – rather than pursuing an academic degree – work toward earning credentials that are needed in the local workforce. Veterans enrolled in CREATES are required to complete strategic internships in public and private sector organizations, with an option to intern as a cybersecurity analyst-in-training. Because the internship curriculum is integrated with the PRISEM/DIMS regional monitoring system, the veteran works as an actual regional analyst, under the direction of the official fusion center analyst, for the duration of the internship. Veterans can also apply for cybersecurity apprenticeships with critical infrastructure systems that are operated by the public sector, such as public utilities, dam operations, water treatment, and irrigation operations. The rotational service of to-be-credentialed practitioners builds the regional workforce while simultaneously addressing resource unavailability in these very important sectors.
    - *Municipal Research and Services Center* – MRSC is a nonprofit organization dedicated to supporting local governments statewide. The Center provides collaborative consultation, research tools, information, training, guidance and facilitation, and access to other shared-service providers to enhance cyber competencies.

IV. PLANNING AND PREPAREDNESS ACTIVITIES

"The impact a cyber event can have on an overall organization necessitates a more holistic and all-encompassing approach to planning and preparedness."

– Samuel J. Boyle, Manager of Emergency Management Services,
Chicago Department of Public Health

IT is being integrated into products, systems, and operations at exponentially increasing rates. IT is now a critical enabler to life safety, essential services, critical infrastructure, and response capabilities. This reliance on expanding cyber dependencies has outpaced its integration with emergency preparedness standards. Over 60 percent of responding *DomPrep* readers said that cybersecurity was not regularly considered in their organizations' preparedness, response, and recovery activities.



NIMS and ICS serve as the U.S. national models for emergency preparedness, planning, and response. Information security professionals, especially in the private sector, are generally unfamiliar with NIMS and ICS; in fact, they currently lack a common crisis management model. Readiness requires a framework for the various technical and procedural response standards, which must be further integrated into the broader crisis management system. Without this shared understanding, uncertainties and inconsistencies abound, leading to potentially disastrous emergency response. Washington State is a national leader in developing strategies to close this divide.

The PLC roundtable discussion highlighted several public and private cyber preparedness deficiencies facing national regions, including:

- Incident command and management structure, roles and responsibilities, and essential practices are not well understood, documented, or routinely practiced.
- Response plans, when they exist, lack maturity or are inadequately exercised.
- Mutual aid agreements either do not exist or face significant barriers.
- Common resource typing and credentialing are not established.
- Cyber and cyber dependencies are not considered in exercise planning and processes.
- Public and private sectors' policy and planning mechanisms are inadequately prepared to support operations in a prolonged loss or denial of services.

An overview of each issue is presented in the discussion that follows. By including information security professionals in planning, exercise activities, and response, the Seattle region and Washington State are actively introducing the local cyber minds to NIMS and ICS. In order to be effectively adopted by the information security community at large, however, the approach must be more broadly promoted, integrated, and evolved.

Incident Command and Management and Systems

Washington State conceived, and continues to develop, a "whole of government, whole of community" strategy to mitigate cyber risks to critical communications, response capabilities, and infrastructure. The Washington Significant Cyber Incident Annex (WSCIA) to the Comprehensive Emergency Management Plan (CEMP) provides a basic coordination framework. Similar to existing emergency management frameworks (which exist within state, local, and tribal governments, as well as within the private sector), the framework provides guidance to operators of cyber-critical infrastructure about how to manage a significant cyber event when it occurs. The WSCIA is built on the foundations of the National Response Framework, the Draft National Cyber Incident Response Plan, and NIMS.

The CEMP includes several unique features. One of these features is the inclusion of defined roles and responsibilities for the homeland security advisor, which are designed to help the advisor coordinate significant cyber incident response. Other features include the creation of the Cyber Unified Coordination Group (UCG), and the charter of a regional public-private information coordinating mechanism (CIRCAS) to "activate" members in the event of an emergency. The UCG consists of carefully selected representatives from federal, state, and local governmental agencies, academia, private

industry, and critical infrastructure sectors. These key stakeholders can quickly acquire resources, authorities, and information for a coordinated response to a significant cyber incident. In the event of a regional disruption event, CIRCAS members are activated to provide advice to the UCG. They provide additional support to ESF2 activities during state emergency operation center activation, and serve as a private sector analog of the mutual aid mechanism that is commonly utilized during emergency operations.

Incident Response Plans

In the cybersecurity world – as in all security fields – a response plan must limit damage, increase the confidence of external stakeholders, and reduce recovery time and costs. Traditional incident response plans provide instructions for responding to a number of potential risks, threats, and failures. They illuminate internal roles and responsibilities, response procedures, service-level agreements, and relationships with third-party providers. Maintaining relationships and accountability with key external partners is an essential design element. Without an established incident response plan, organizations might be unable to detect an attack in the first place, or may lack proper protocol to contain and recover from the threat once it is detected.

Discussions during the PLC roundtable addressed a breadth of regional inconsistencies in planning and exercise. In the planning realm, incident response plans often do not exist. When they do, they are insufficiently developed or operationalized, or have not been integrated across governmental or business units. When discussing how plans should be better exercised, the PLC members noted the need for response plans to be tested and evaluated, on a regular basis, against diverse requirements (from optional requirements, to those mandated by regulations). All parties agreed that an effective incident response plan ultimately relies on established executive sponsorship, well-developed policies for operations and procedures, and enterprise-level testing that takes into account dependencies and interdependencies. Additionally, while the roundtable attendants did not reach a consensus, much discussion focused on trigger points for response plans. They discussed various approaches to establishing and accurately communicating trigger-point alerts between various participants – including when and how the state cybersecurity emergency plan should be activated. They agreed that stakeholders need a more common understanding in this area.

Cyber Mutual Aid Agreements

Mutual aid agreements are the foundation upon which cross-jurisdictional, cross-corporate disaster and emergency assistance is built. Very few, if any, cybersecurity mutual aid agreements exist. Although state, tribal, and local governments, as well as the private sector, routinely provide emergency assistance to one another, mutual aid

structures and mechanisms to support cyber response are not clearly understood or developed. Without common understanding by all involved parties, communication is ineffective and can hinder response efforts. Mutual aid agreements can pose many benefits to the IT and cyber worlds, including increased timely access to critical resources (e.g., personnel, equipment, and incident-specific expertise), professional solidarity (the appropriate resources provided to affected communities), and public reassurance that essential services will return quickly.

Unlike in other emergencies, cyber incident response has a unique dependence on third-party organizations (contracted expert service). Most organizations do not internally maintain the level of IT expertise needed to fully respond to or recover from cyberthreats. Though there have been regional efforts to develop cyber mutual aid agreements, these efforts have stalled; the cross-sector communities use disparate resource typing definitions and operate under different legal liability and indemnification agreements (both as they apply to individuals and organizations). Without a common language or understanding in these areas, an effective mutual aid response cannot be established. In the interim, CIRCAS is working on the first step: creating mutual aid responders who can act as liaisons to bridge the mutual aid gap. These responders are carefully vetted individuals who have a standing agreement to provide advice, analysis, and response for those events that exceed the response capabilities of a member organization.

Resource Typing and Credentialing

Public and private sector information security professionals must also develop a common understanding of critical resources before an event; they must understand the type of resources available, and how those resources can be accessed and shared. This is especially critical in IT systems, given the systems' complexity and specializations. As previously discussed, it is necessary to establish common resource typing and related language in order to effectively communicate within and between the governmental and private sectors. Just as diverse teams must come together under a common understanding to respond to a physical incident, successful cyber response must integrate first responders with diverse competencies and capabilities. Necessary parties include those with technical and nontechnical key skill sets, such as the private sector legal community. Legal and administrative support is required to perform internal and external legal coordination, determinations, and notifications. Without common resource typing, mutual aid agreements cannot be established (this topic is discussed in further detail in the next chapter). The National Guard is working toward a solution, and has initiated and focused on Tier-2 (state-level) resource typing, indemnification for volunteer responders, and credentialing. This solution leverages and is in collaboration with the CIRCAS mutual aid efforts.

Cybersecurity roundtable discussion, Seattle, WA.

Exercise Strategies

Exercises enable participants to identify strengths, illuminate the best practices for sustaining and enhancing existing capabilities, and objectively assess gaps and shortfalls within plans, policies, and procedures. Information technology, a connective capability, should be an integral component to all planning and preparedness activities. In many instances, however, planners consider IT security and resilience as separate or standalone exercises. The Seattle region is establishing a culture in which cybersecurity is essential to the exercise planning process. This more inclusive approach has indoctrinated enhanced organizational and regional awareness and identification capabilities. Further, it has established planning activities that account for systems and network dependencies, third-party dependences (including third-party cyber risks), and mutual reliance on common vendors and service providers and time-critical equipment.

Communication, Planning, and Contingency Operations

The cyberworld is highly competitive, and utilizes complex resources. Security can be easily overshadowed by competing priorities and needs. Senior cyber leaders must be able to effectively communicate cyber-related risks, impacts, and budget and investment implications in this complex environment. The annual "2014 Deloitte-NASCIO Cybersecurity Study" found a continuing significant divide between information technology professionals and elected officials on the confidence, integrity, resilience, and availability of security-critical systems.[8] Technologists and preparedness communities must mutually develop better strategies to discuss, educate, and promote resilience and cyber-risk preparedness, up to and including continuity of operations. Currently, the majority of public and private sector organizations' contingency plans – as well as those for the general public at large – assume availability of broadband and system access from a residential, environment, or geographic region. Both sectors are inadequately prepared to support operations in a prolonged loss or denial of services.

V. POLICY FRAMEWORK ISSUES

"Cyberattacks could happen at anytime, anywhere. We need a federal/state template on how to prevent an attack."
– Jay Hammes, President and Founder, Safe Sport Zone, LLC

In *The Fifth Discipline: The Art & Practice of the Learning Organization*, Peter Senge's first law is "today's problems come from yesterday's solutions."[9] The problems inherited today are the result of inventions, breakthrough products and services, and solutions to past shortfalls and challenges. True to this law, ever-increasing advanced capabilities and interconnected systems require new policies and procedures to reduce confusion and risk. The threat of a cyberattack is persistent and increasingly sophisticated. As the pace of change and threats continue to increase, so must collaborative policies and mitigation practices.

The PLC roundtable highlighted several significant IT and cyber-driven policy challenges altering current preparedness, response, and recovery framework areas. These challenges include: (a) the disaster assistance framework; (b) incident management for IT professionals; (c) resource typing and credentialing; (d) legal barriers and risks; (e) the National Guard's authorities; (f) sustainability and resourcing of regional capabilities; and (g) technical and administrative enabling of information reporting. A short discussion on the each of these issues follows.

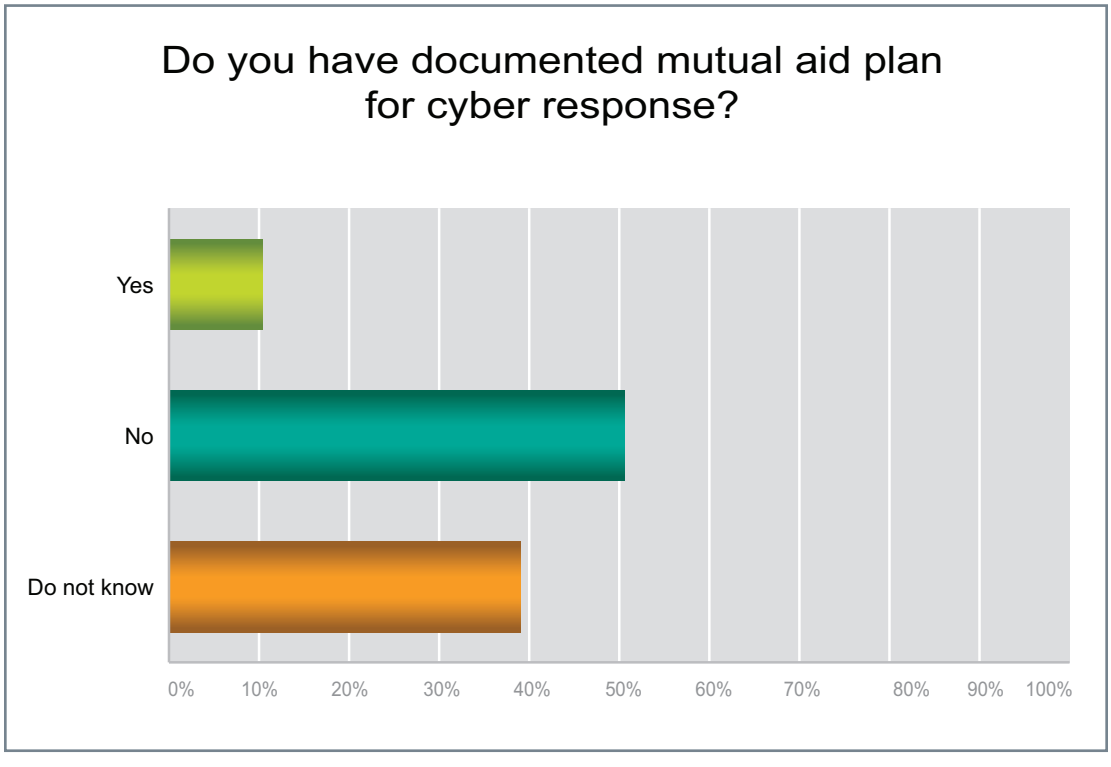
However, two significant policy issues underpin each of these individual areas. First, individuals with operational or requirements experience need to be part of information security and cyber policy development. In many cases, policy development is led and dominated by individuals with limited technical experience or operational understanding of the significant issues, dependencies, and legal and business restrictions. Second, effective policy development in the cyberspace is dependent on public and private sector collaboration. Washington State's unique environment and collaborative processes have the potential not only to resolve some of these issues locally, but also to significantly contribute to the development, harmonization, and enactment necessary to effect policy changes on a much broader level.

Disaster Assistance Framework

The federal Stafford Act and state-level EMAC are the significant existing policy frameworks governing systematic, orderly disaster assistance. Nationally, these strategies were created to encourage states and localities to develop comprehensive disaster preparedness plans, prepare intergovernmental coordination in the face of a disaster, utilize insurance coverage, and provide assistance programs for disaster-related losses.

These frameworks also ascribe the public sector a prominent role in planning and response activities – public organizations are charged with promoting preparedness, risk management, and resilience.

Neither policy framework, however, truly accommodates the private sector's significant role with daily IT operations and cybersecurity, or the public sector's dependency on these private sector resources and capabilities. They do not reflect how much individual companies depend on resources and cyber competencies housed in other organizations – especially resources that are needed for major cyber incident response. Further, the frameworks do not address the multiple dependencies and interdependencies that crosscut the public and private sectors. Although the Stafford Act provides a clear framework for public sector lead agencies' physical emergency response, no analog clarifies authorities and policies to provide necessary and integrated assistance during IT-related disasters and emergencies. This absence inhibits greater cyber preparedness and response and is well beyond the influence of these regional framework discussions. Alternatively, the regional efforts, if coordinated via state emergency management leaders, can effectively promote EMAC revisions and recommendations to better facilitate the maximum use of all available resources within member states and the private sector.



Incident Management

When asked if their organization had a documented mutual aid plan for cyber response in place, 50 percent of responding *DomPrep* readers said, "No"; and nearly 40 percent were unsure. Information security professionals need a standard crisis management model that provides not only an industry-focused framework for the various technical and procedural standards, but also one that integrates that framework into a national system.

ICS is the preeminent, tried-and-true crisis management system that serves to integrate cyber preparedness and response. Among its many attributes, ICS: supports event scalability; provides integration to those leading the incident response with operations, planning logistics, and finance/administration capabilities; and enables known access methods to skills and resources. Regional policymakers should ensure that information security professionals promote, adopt, and include ICS standards into their planning processes.

Resource Typing and Credentialing

In IT operations, certainty is critical. As previously mentioned, precision and accuracy are needed to support physical and logical operations, and to monitor both day-to-day operations and ongoing incidents. Information security professionals need to develop and document a series of common understandings that span the public and private sectors. Namely, critical resources – including resource typing, awareness, access and sharing, and legal agreements – must be commonly discussed before an event. Common resource typing is the first step toward establishing the common language necessary for effective communication within and between governmental and NGOs. Given the private sector's dominance in certifications, commercial certifications should be included within resource typing requirements.

There must also be an established policy for digitally identifying and authenticating the people responsible for these critical actions. Before work begins, stakeholders must commonly confirm that these individuals are who they claim to be, and that they possess the competencies, skills, certifications, or permissions they claim to possess. Multifactor authentication is an increasingly common requirement, and should be considered within the common regional policy development. FIPS-201-based credentials provide one such common interoperability between all federal personnel, National Guard members, and Transportation Worker Identification Credentials holders (individuals in the Coast Guard operating within Maritime Transportation Security Act areas). A FIPS-201-based/PIV-I identity framework provides interoperability with federal credential efforts and resources, and aligns with trusted framework efforts at the federal level. This scalable framework is interoperable across multiple federated trust frameworks already deployed in the defense-aerospace, bio-pharma, and banking and finance communities.

Legal Barriers and Risks

It is abundantly clear that, in many respects, an organization's level of cybersecurity is only as good as the cybersecurity of its vendors. If an organization is unable to identify, monitor, and mitigate risks posed by its third-party relationships, a response plan may be too little too late. The cybersecurity professionals at the roundtable meeting discussed approaches to establishing third-party minimum requirements. They agreed that organizations should question their vendors' information security practices, and how the related requirements extend to their subcontractors. For example, questions posed to third-party vendors could include:

- What are your policies regarding disclosure of information, anonymity of data, privacy protection, or other issues that could affect your organization's liability?
- How do you notify all concerned parties in the event of an information or other security breach?
- Do you conduct, or allow a constituent organization to conduct, onsite assessments?
- Do your data or products have an integrity warranty? Do you ensure that they are free of viruses and will remain so?

Long-term policy commitment is required to prioritize, establish resolution framework, and develop agreement solutions and support their enactment.

National Guard Authorities and Roles

Authorities and roles have significantly changed in recent years. This rapid evolution has introduced uncertainty and risk issues for the National Guard as well as the private sector. State governors have traditionally activated National Guard personnel to State Active Duty (SAD) in response to natural or manmade disasters, or for homeland defense missions. The 2010 National Defense Authorization Act allows designated National Guard officers – Dual-Status Commanders – to command forces under both Title 10 and Title 32 statuses. A key aspect of this duty status is that the Posse Comitatus Act does not apply, giving National Guardsmen the ability to act in a law enforcement capacity within their home state or adjacent state, if granted authority by that state's governor. Since 2014, governors have had the ability to employ National Guard cyber-trained personnel in Title 32 status to provide state-initiated and state-directed cyber support to civil authorities. Consistent with federal and state law, the Guardsmen thus serve as experts certified to coordinate, train, advise, and assist local stakeholders.

In conjunction with their governors and the secretary of defense, adjutant generals of each state, territory, and district are trying to determine the risks and appropriate engagement requirements of the cyber mission for both the public and private sectors. Policies and guidelines need to be further clarified in order to support more consistent and effective mission execution, and to improve the National Guard's pre- and post-event coordination with local cyberspace operations. Within the private sector, especially in the technical and intellectual property community, there are legal liabilities and risks of exposing activated or competitive employees to sensitive and proprietary information; once they are exposed to this information, they cannot simply "unknow" it. Private-sector participation and acceptance requires additional legal clarification or legislation.

Sustainability and Resourcing of Regional Capabilities

Not-for-profit and public-private partnership organizations play a significant sustainability role in Washington State; they provide shared services and capabilities critical to the region's success. For example, Agora and CIRCAS actively promote education, awareness, and coordination through the public-private-sector divide, and they support system resources. It is essential that other regions utilize NGOs and public-private partnership strategies to establish long-term sustainment, which includes incorporating established resourcing models and succession strategies.

Enabling Technical and Administrative Information Reporting

Common technical and administrative policies are essential to effective information sharing. In some sectors, information being shared or monitored is subject to public disclosure. To overcome this, many private sector organizations use trusted NGOs to share information, thereby avoiding potential liabilities or restrictions. An optimal policy is one that promotes real-time, anonymous information sharing; corroborating the information helps protect all parties' reputations, strengthens awareness, and promotes action. This creates a more holistic approach to regulatory compliance and information sharing as part of the cyberstrategy.

KEY FINDINGS

Unique Regional Collaborative Traits

- Cybersecurity is a leadership priority shared by the political and public safety communities in the Washington State region. It is supported organizationally and in policy and operations.
- Greater concentration between public and private leadership and workforce who possess cybersecurity competence – including design-build and operational experience – increases a region's overall competence.
- Strong regional relationships depend on successful interactions between public and private sector individuals involved in infrastructure protection, workforce development, and educational and academic research strategies and polices.
- Active executive-level support for, participation in, and trust in not-for-profit and public-private partnerships support regional cyber focus, capabilities, and relationships.
- Shared-service strategies help provide cyber competency and capabilities to support traditionally under-resourced areas of the public sector, including local government and publically managed critical infrastructure.
- The IT and cyber communities are gaining an increasing understanding of ICS/NIMS concepts, helping them to develop comparable strategies for cybersecurity.
- Cyber policies and issues must be integrated into all exercises and planning activities.

Common Understanding

- Cybersecurity should be viewed and communicated as a matter of public safety and economic issue. It affects the worth of goods and services, as well as the protection of intellectual and proprietary property.
- Regional cyberstrategies rest on building and renewing strong interpersonal relationships, and bringing the right public and private sector stakeholders to the table to share information and resources.

- Communication and information sharing depend on trusted formal and informal support structures. This includes routine in-person exchanges, at both the executive and operational levels, and the ability to electronically share information at various levels of risk and access.
- Information sharing must occur and flow between all levels of participants, with contributors' efforts being recognized and reciprocated.
- Critical infrastructure and key resources, especially life and safety systems, have more serious vulnerabilities, and therefore priority needs, than commercial and business organizations.
- Trust must be inherent in formal and informal information-sharing mechanisms.

Information-Sharing Structures and Mechanisms

- Formal and informal mechanisms for information sharing already exist within and across federal, state, local, and tribal governments, as well as the private sector.
- Information sharing and communication primarily occur within sectors and related organizations, and within professional disciplines. There are limited cross-sector and cross-discipline processes for regional information sharing. Not-for-profit and public-private partnerships can effectively serve as trusted third parties, bridging these critical gaps.
- Existing information-sharing organizations and mechanisms should not be perceived as competing, or as an excuse for mandated mechanisms. Instead, they should be considered channels of choice supporting sector, community, and individual choices of priorities, preferences, and needs.
- Effective information sharing includes layers for: executives; direct management and operators; monitoring, detecting, and securing sensitive information; and response systems.
- Organizations are dependent on trusted and time-sensitive analytical capabilities and exchanges. These capabilities are shared among public and private sector participants.

Planning and Preparedness Activities

- Incident command structures, roles and responsibilities, and practices to support cyber incidents are not well understood or routinely practiced.
- Mutual aid structures and mechanisms to support cyber response are not clearly understood or developed.
- Resource typing provides a common language and understanding critical to communication, information sharing and analysis, preparedness, and response.
- Authentication of credentials and attributes is critical in physical and logical operations. Communities lack a common definition of authentication approaches to verify that people are who they claim to be and that they possess the competencies, skills, certifications, and permissions they claim to possess.
- Cyber needs and dependencies should be considered within all exercise planning and development activities as a matter of course.
- Organizations need to identify and be aware of the risks associated with third-party dependences. There is a high variation and certainty of security integrity and response availability (especially during a regional event) of third-party vendors and service providers.
- ITechnology and preparedness communities must unify their efforts to discuss, educate, and promote resilience and preparedness for cyber risks – up to and including continuity of operations.
- The public and private sectors are inadequately prepared to support operations in a prolonged loss or denial of services.

Policy Framework Issues

- Absence of a Stafford Act analog – which would clarify authorities to provide necessary and integrated public and private sector assistance during declared major disasters and emergencies – inhibits greater cyber preparedness and response.
- EMAC must be revised to better facilitate the maximum use of all available resources within member states and the private sector.

- Significant legal barriers to regional cyber planning, response, and recovery include: liability, safe harbor, privacy protection, and warrantee issues. Long-term policy commitment is required to prioritize, establish a resolution framework, and develop agreement solutions and support their enactment.
- Long-term sustainability and resourcing of "trusted" not-for-profit and public-private partnerships must be established.
- Common public and private sector policy for supporting integrated major disaster or emergency response – as it involves cyber or IT infrastructure – does not yet exist. Key issues include: credentialing and resource typing of individuals, capabilities, and their authentication; awareness, access to, and sharing of resources, including capabilities and long-lead items; and legal agreements supporting and enabling mutual aid.
- Technical and administrative policies are needed to strengthen awareness and actionable information sharing. Examples include promoting anonymity of information reporting, reputation scoring, and corroborating information.

ACTION PLAN

Recommendations for Action

1. Revise EMAC to facilitate the maximum use of all available resources – within member states' public and private sectors – that are unique and necessary to support response to a major event.
2. Support awareness and adoption of ICS/NIMS concepts within the cyber community. Comparable strategies for cybersecurity and response should be developed and reflected in cyber annexes to response plans.
3. Develop and sustain effective partnerships between public and private organizations. In doing so, allow not-for-profit and other private entities to serve as trusted third parties that bridge cross-sector and cross-discipline processes and mechanisms. Partnerships should promote regional relationships, information sharing, and coordination of processes (e.g., PNWER, CIRCAS).
4. Include IT system availabilities, dependencies, and interdependencies and cyber impacts in exercise planning and development as a matter of course. Exercises should consider system failure points, third-party product and service providers, and continuity of operations (including viability of telework and remote access from an external environment impacted by a cyber event).
5. Develop and document a common public and private understanding of critical resources. Resources should clarify common language, resource typing, awareness, access and sharing, and legal agreements before an event.
6. Develop common policy for authentication of credentials, attributes, and claims for physical and logical operations. The policy should support interoperability and multifactor digital authentication to confirm that individuals are who they claim to be and they possess the competencies, skills, certifications, and permissions they claim to possess.
7. Refine and support information-sharing mechanisms across executive and operational levels. Mechanisms should take into account various levels of risk and have capabilities for support monitoring, detection, sharing of sensitive and secure information, and sharing of response information (for example, PIECES, RECAP, DIMS).
8. Promote definition and adoption of common contract language or requirements addressing security and integrity of third-party product and service providers.
9. Support and further enhance cyber shared-service and managed-service strategies. These strategies provide access and affordability of cyber competency and capabilities to traditionally under-resourced entities. They also address traditional vulnerabilities and strengthen federated resilience and operations.

LIST OF ACRONYMS AND ABBREVIATIONS

CERT	Computer Emergency Readiness Team
CIRCAS	Cyber Incident Response Coalition and Analysis Sharing
DIMS	Distributed Incident Management System
EMAC	Emergency Management Assistance Compact
ICS	Incident Command System
IPT	integrated project team
ISAC	Information Sharing and Analysis Centers
ISAO	information sharing and analysis organization
IT	information technology
NCCIC	National Cyber security Communication and Integration Center
NGO	Nongovernmental organization
NIMS	National Incident Management System
PISCES	Public Infrastructure Security Collaboration and Exchange System
PLC	Preparedness Leadership Council International
PNWER	Pacific Northwest Economic Region
PRISEM	Public Regional Information Security Event Monitoring
RECAP	Regional Economic Cyber Analytics Platform
UCG	Cyber Unified Coordination Group
WSCIA	Washington Significant Cyber Incident Annex
WSFC	Washington State Fusion Center

ENDNOTES

[1] Obama, Barrack. *Promoting Private Sector Cyber Security Information Sharing* (Executive Order 13691). Washington, DC: The White House, February 13, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[2] Department of Homeland Security. "Information Sharing and Analysis Organizations (ISAOs)." Last modified April 13, 2016. https://www.dhs.gov/isao

[3] Porter, Michael E. *Clusters of Innovation: Regional Foundations of U.S. Competitiveness.* Washington, DC: Council on Competitiveness, 2001. http://www.compete.org/storage/images/uploads/File/PDF%20Files/CoC_Reg_Found_national_cluster.pdf

[4] Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime (Economic Impact of Cybercrime II).* Santa Clara, CA: Intel Security, 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[5] U.S. Census Bureau. "State Exports from Washington." Last modified December 12, 2015. https://www.census.gov/foreign-trade/statistics/state/data/wa.html

[6] Washington Military Department. *Washington State Significant Cyber Incident Annex to the Washington State Comprehensive Emergency Management Plan* (Annex D). The State of Washington, March 2015. http://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

[7] Washington State Fusion Center. "About the Washington State Fusion Center." Accessed April 20, 2016. http://www.wsfc.wa.gov/About

[8] Deloitte and the National Associateion of State Chief Information Offers (NASCIO). 2014 *Deloitte-NASCIO Cybersecurity Study–State Governments at Risk: Time to move Forward.* New York: Deloitte Development, 2014. http://www2.deloitte.com/us/en/pages/public-sector/articles/2014-deloitte-nascio-cybersecurity-study.html

[9] Senge, Peter M. *The Fifth Discipline The Art & Practice of the Learning Organization.* New York: Currency Doubleday, 1990.

APPENDIX A
PLC Cybersecurity Roundtable Participants

Chris Aardahl	Director, Homeland Security Programs	Pacific Northwest National Laboratory
Thad Allen	Executive Vice President	Booz Allen Hamilton
Peter Chiou	Principal Engineer	Microsoft
Scott David	Director of Policy	Center for Information & Cybersecurity, University of Washington
Dr. Barbara Endicott-Popovsky	Executive Director	Center for Information & Cybersecurity, University of Washington
Jon Engstrom	Detective	Seattle Police Department
Robert Ezelle	Director	Washington State Emergency Management Division
Christina Flowers	U.S. Sales Account Manager	BioFire Defense
Chris Grant	CISO	Group Health Cooperative
Alisha Griswold	Emergency Manager	King County Government
Michael Hamilton	Policy Advisor	Washington State Office of the CIO
Scott Klauminzer	Critical Infrastructure Protection Lead	Tacoma Public Utilities
Darren Kress	Director, Security Solutions	T-Mobile
Dave Lemanowicz	Sr. Incident Coordinator	Cyber Defense Operations Center, Microsoft IT
Ann Lesperance	Director Regional Programs	Pacific Northwest National Laboratory
Tim Lowenberg	Major General (Ret.), Vice President	Gordon Thomas Honeywell Governmental Affairs
Jessica Matlock	Director, Government Relations	Snohomish County PUD
David Matthews	Senior Associate	MK Hamilton & Associates
Russ McRee	Director, Security Response & Investigations	Microsoft/OSG
Matthew Modarelli	Cyber Security Manager	Washington State Emergency Management Division
Thomas W. Muehleisen	LTC, IN (FA30/53) WAARNG, Lead Cyber Planner	Washington National Guard
David Olive	Principal	Catalyst Partners

(continued)

PLC Cybersecurity Roundtable Participants

Vayl Oxford	National Security Advisor	PNNL
Kierra Phifer	South Sound Regional Director	U.S. Senator Patty Murray
Amelia Phillips	Chair, Pure & Applied Science Division	Highline College
Jesse Rieth	National Security Advisor	U.S. Attorney's Office, WDWA
Jodie Ryan	Sr. Incident Response, Cyber Defense Operations Center	Microsoft
Rob Schnepp	Division Chief of Special Operations (Retired)	Alameda County Fire Department, CA
Mark Smith	Principle Security PM	Microsoft Corporation
Tom Snead, Sr.	Incident Coordinator	Cyber Defense Operations Center, Microsoft IT
Lori Sparks	Principal	Booz Allen Hamilton
Steve Stein	Director	Pacific Northwest National Laboratory
Grant Tietje	Director of Programs	Northwest Healthcare Response Network
Selena Tonti	CISO	Port of Seattle
Andy Tuck	Director, Infosec Operations & Engineering	Costco Wholesale Inc.
Ron Vidal	Partner	Blackrock 3 Partners
Tim Wise	Information Security Engineer	Snohomish County

APPENDIX B
Contributors

Ann Lesperance, Director,
Northwest Regional Technology Center,
Pacific Northwest National Laboratory

Jim White, Public Safety Clinical Lecturer,
School of Public and Environmental Affairs
Indiana University, Purdue University,
Indianapolis

Matt Modarelli, CIO & Director,
Information Technology Division,
WA Military Department

James Horn, Ranger/SF RPD

Matt Miller, CEM Texas Engineering
Extension Service

Alan B. McCoy, Assistant Public Health
Emergency Coordinator,
City of Gary, Indiana Health Department

Frances L. Edwards, Director,
National Transportation Safety and
Security Center,
Mineta Transportation Institute,
San Jose State University

Gary Rapelje, Regional Coordinator,
Region 7 Healthcare Coaltion

Mark Schultz, Executive Coordinator for the
Strategic National Stockpile Emergency
Preparedness and Response Service,
Oklahoma State Department of Health

James A. Williams, IT Specialist

Tom Muehleisen, Lieutenant Colonel,
Infantry J36 Cyber Operations,
Washington National Guard

David R. Matthews, Chief Mindfullness Officer

Don Wyatt, RN

Jim Garrett, Intelligence Analyst,
Missouri National Guard

Jeff Gerald, CEO, Gray Matters, Inc.

Lori Stoney, Battalion Chief,
Homewood Fire & Rescue Service

Matthew Cern, Zone Coordinator,
Summit County, Ohio
Fire/EMS, Valley Fire District, Ohio

Marie Shadden, MPA Consultant, Water Security

Kathleen Berlin, Medical Reserve
Corps Coordinator,
University of Minnesota Academic Health
Center Office of Emergency Response

Patrick Moore, LTC (Retired), U.S. Army
AMEDD

Captain James Henning, Chief Deputy,
Caroline County Sheriff's Office, Maryland

Warren Lee, Director, New Hanover County
Department of Emergency Management

Robert A Mitchell, CFO, CEMSO, FPEM
Assistant Fire Chief / EM
Reedy Creek Fire Dept. Planning Section
Chief – NDMS & FL Region 5 IMT

Don Wilkinson, Local Emergency
Response Coordinator,
Oklahoma State Department of Health

Lee Trevor, RN, CPIINS, CHEP
Clinical Educator,
Disaster Preparedness Coordinator,
TriStar Summit Medical Center

Steve Pappas, Owner, Pappas Associates, LLC

Lisé Crouch, Coordinator,
Hendricks County, Indiana EMA

David Breeding, Director,
Claiborne County Government Office of
Emergency Management Homeland Security

(continued)

Contributors

Ray Pena, Professional Emergency Manager, Self employed

David Reddick, Business Continuity-Disaster Recovery Coordinator, Saint Louis University

Gerald Gifford, Emergency Preparedness Manager, East Metro Health District 3-4

Gordon Hunter, Operations Evaluator, National Guard Bureau Standardization Evaluation Assistance Team Chenega Applied Solutions

Brendan McCluskey, Director, Emergency Preparedness & Operations Division of Public Health Infrastructure, Laboratories, and Emergency Preparedness, New Jersey Department of Health

Andrew Reeve, Chief Technical Officer

Linda Langston, Linn County Supervisor, Linn County, Iowa, Past President National Association of Counties

Vivienne Treharne, B.S.N., R.N., Registered Nurse Consultant Responder Safety and Health and Disaster Behavioral Health Program Manager, Florida Department of Health Bureau of Preparedness and Response

Peter F. Gruen, RN Public Health Nurse, Erie County Department of Health Office of Public Health Emergency Preparedness

John J. Burke, Deputy Fire Chief, Sandwich Fire Department

Joe LaFleur, Manager, Corporate Crisis Management / Business Continuity / IT Disaster Recovery

Joe Manous, Institute for Water Resources, U.S. Army Corps of Engineers

Marc Barbiere, Emergency Management Coordinator, Fairfax County Health Department

John Contestabile, Program Manger, Emergency Preparedness and Response Systems, Johns Hopkins University/Applied Physics Lab

Christopher Godley, Director of Emergency Management, Tetra Tech

Vivian A. Marinelli, Psy.D. Senior Director, Crisis Management Services FEI

Robert J Fink, Emergency Management Specialist, County of Bucks

David N. Gerstner, MMRS Program Manager, Dayton Fire Department, Dayton, Ohio

Jeffrey W. Runge, MD, National Collaborative for Bio-Preparedness, The University of North Carolina at Chapel Hill

Samuel J. Boyle, Manager of Emergency Management Services, Chicago Department of Public Health

Zsolt Szoke, Captain, Charleston Fire Dept., SC

Michael Jarvis, Police Officer, Nebraska

Walter Harris, Contract Officer, DISA

David J. Miller, Jr., MPH, FRSPH, CPH, CHS-I, CHSO, AEMT-CC Coordinator, Emergency Management Services Department of Emergency Management, IMC Operations Interfaith Medical Center

Jay Hammes, President and Founder, Safe Sport Zone LLC

APPENDIX C
Preparedness Leadership Council

Executive Committee:

Marko Bourne
Principal, Booz Allen Hamilton (BAH)

Stephen Reeves
Major General USA (Ret.)

Martin Masiuk
President, IMR Group Inc., Publisher of DomesticPreparedness.com

James Schwartz
Chief, Arlington County Fire Department

Vayl S. Oxford
National Security Executive Policy Advisor, Pacific Northwest National Laboratory (PNNL)

Robert (Bob) Stephan
Executive Vice President, CRA Inc.

Kenneth P. Rapuano
Senior Vice President and Executive Director Homeland Security Group, The ANSER Corporation

Craig Vanderwagon, M.D.
Senior Partner, Martin Blanck, and Associates

Policy Committee:

Elizabeth B. Armstrong
Chief Executive Officer, International Association of Emergency Managers (IAEM)

Linda Langston
President, National Association of Counties (NACo)

Asha G. George, Ph.D.
Co-Director for the Blue Ribbon Study Panel for Biodefense and Principal at Strategic Operational Solutions

John Morton
Senior Strategic Advisor

Cybersecurity Working Group:

Michael K. Hamilton
Chief Executive Officer and Managing Partner, MK Hamilton & Associates

Lori Sparks
Principal, Booz Allen Hamilton

David R. Matthews
Founder, Cyber Incident Response Coalition and Analysis Sharing Group

Steven L. Stein
Director, Pacific Northwest National Laboratory

Matthew Modarelli
Cyber Security Manager, Washington State Emergency Management Division

Kelly Woods Vaughn
Managing Director, Infragard National Members Alliance (INMA)

David M. Olive
Founder & Principal, Catalyst Partners LLC

Colonel Gent Welsh
Chief of Staff, Washington Military Department & Washington National Guard

Preparedness Leadership Council Members

Members:

Amy L. Altman, Ph.D.
Vice President,
Biodefense, Luminex

James J. Augustine, M.D.
Emergency Physician, Clinical Associate Professor, Department of Emergency Medicine, Wright State University

William Austin
Homeland Security Coordinator,
Connecticut Capitol Region
Council of Governments

Ellen Carlin
Principal,
Carlin Communications

Megan Clifford
Deputy Director,
Infrastructure Assurance Center,
Argonne National Laboratory

Kenneth W. Comer, Ph.D.
Associate Professor, George Mason University

John Contestabile
Assistant Program Manager,
Homeland Security, Johns Hopkins University/Applied Physics Lab

David W. Cullin, Ph.D.
Vice President, Research,
Development & Programs,
FLIR Systems Inc.

Craig DeAtley
Director, Institute for Public
Health Emergency Readiness,
MedStar Washington Hospital Center

Christina M. Flowers
U.S. Sales Management and
Business Development,
BioFire Defense

Kay C. Goss
Chief Executive Officer,
GC Barnes Group LLC

Charles J. Guddemi
Federal Law Enforcement Officer

Douglas Kinney
Business Continuity/Continuity
of Operations Consultant,
BDA Global LLC

Michael G. Kurilla, M.D., Ph.D.
Director, Office of BioDefense,
Research Resources,
National Institute of Health

Thomas J. Lockwood
Senior Associate,
Professional & Executive Services LLC

Anthony S. Mangeri, Sr.
Manager of Strategic Relations for Fire Services & Emergency Management,
American Public University System

Heather Medwick
CEO for the International Centre
for Infectious Diseases

Robert Miller
Divisional Director: U.S. Federal
Government Programs,
Draeger Inc.

David M. Olive
Founder & Principal,
Catalyst Partners LLC

Gerald W. Parker, DVM, Ph.D., MS
Vice President, Public Health
Preparedness and Response,
Texas A&M Health Science Center

Preparedness Leadership Council Members

Members:

Joseph Picciano
Deputy Director for Preparedness, New Jersey Office of Homeland Security & Preparedness

Jeff Runge
Managing Member, Vigilant LLC

Justin Snair
Program Officer, Board on Health Sciences Policy, Health and Medicine Division, National Academy of Sciences, Engineering, and Medicine

Susan Snider
Executive Director of the Northern Virginia Hospital Alliance

Maureen Sullivan
Supervisor, Emergency Preparedness and Response Laboratory Unit, Minnesota Department of Health Public Health Laboratory (MN-PHL)

Mike Wernicke
Vice President, Commercial Development & Operations, Emergent BioSolutions Inc.

Thomas K. Zink, M.D.
Associate Professor, Environmental & Occupational Health, Institute for Biosecurity, Saint Louis University

APPENDIX D
Demographics of DomPrep Readers

In what sector are you employed?	
Sector	Percentage of Responses
Public Health	14.37%
Emergency Management	11.56%
Fire Service	11.25%
State/Local Government	11.25%
Hospital (including VA)	8.75%
Federal Government	8.13%
Academic Institution	6.88%
Law Enforcement	5.31%
Privately Owned Company	4.69%
Responses	3.75%
EMS	3.13%
Publicly Traded Company	2.81%
Non-Government Organizations	2.50%
Self-Employed	2.50%
Military	2.19%
Student	0.63%
Elected Office/Legislative Body	0.31%

What type of position do you hold?	
Answer Choices	Percentage of Responses
Upper Management	19.16%
Middle Management	30.24%
Operations	25.45%
Technical	6.29%
Training	4.49%
Administration	3.89%
Appointed	1.80%
Other	8.68%

"I have been taught by senior national security officials for decades never to bring them a problem without also suggesting a solution."

– Richard A. Clarke
Cyberwar: The Next Threat to National Security & What to Do About It

UNDERWRITERS