More Intelligent, More Effective Cybersecurity Protection

January 2013

Business Roundtable (BRT) is an association of chief executive officers of leading U.S. companies with more than $7.3 trillion in annual revenues and nearly 16 million employees. BRT member companies comprise nearly a third of the total value of the U.S. stock market and invest more than $150 billion annually in research and development — equal to 61 percent of U.S. private R&D spending. Our companies pay $182 billion in dividends to shareholders and generate nearly $500 billion in sales for small and medium-sized businesses annually. BRT companies give more than $9 billion a year in combined charitable contributions.

Copyright © 2013 by Business Roundtable

More Intelligent, More Effective Cybersecurity Protection

Table of Contents

Executive Summary 1

I. Background 3

II. Proposal 5

III. Conclusion 15

Appendix A: Sector-by-Sector Cybersecurity Activity 16

Appendix B: Proposal — Summary of Government and Company Commitments 22

Executive Summary

Cybersecurity threats from nation states and other well-funded, highly motivated actors present risks that neither the public nor the private sector can unilaterally address. Formidable criminals are systematically stealing intellectual property through cyber theft. Even more dangerous adversaries are developing tools and capabilities to disrupt critical services that support the world's economy, security and public safety. Shared threats of this magnitude require unprecedented levels of public-private collaboration to successfully defend against them.

To that end, the single most important element of an effective cybersecurity policy is information sharing. Without timely and actionable information about threats, companies can only speculate about which risks are greatest. Effective information sharing is not only an exchange of threat information but also a robust set of trusted, well-structured and regularized policies and processes among the U.S. government, international allies and private-sector entities. Effective information sharing includes the two-way exchange of alerts, response actions, situational awareness and mitigation analysis.

However, instead of focusing on information sharing and collaborative risk management, government proposals misdirect scarce public and private-sector resources to compliance-based, check-the-box models. These proposals place the cart before the horse by calling for government creation of cybersecurity practices and standards before much-needed information sharing legislation is passed and implemented. Ultimately, these compliance-based solutions would fail to create an adaptive and collaborative structure that would allow the public and private sectors to advance risk management models capable of managing cybersecurity threats as they continue to evolve.

To effectively address the risks presented by cybersecurity threats, Business Roundtable has developed a cross-sector approach that can mature and strengthen over time and that will also improve the nation's ability to identify gaps and measure progress. This approach — premised on our *Mission Critical* principles[1] — calls for public and private-sector commitments covering:

[1] For more information on *Mission Critical,* see: http://businessroundtable.org/studies-and-reports/mission-critical.

- **Information Sharing:** We support legislation that creates robust, two-way information sharing, with appropriate legal and privacy protections, between government and the private sector to exchange the specific threat information that will allow both government and business to better secure the nation's cyber assets and mitigate emerging threats in real time. The government must create a clear and concise legal framework for both private sector to private sector and private sector to public sector sharing, with appropriate liability, antitrust and freedom of information protections for those acting within the framework. All of the actions we propose depend on the advancement of information sharing and removal of current legal barriers.

- **Threat-Informed Risk Management:** Once cyber threat information is readily shared between the public and private sectors, it will be necessary to expand existing efforts to develop threat-informed risk management and mitigation methodologies. To accomplish threat-informed risk management, new policies must build on existing sector coordinating councils and government operations centers and must position senior public and private-sector leaders to collaboratively oversee cybersecurity efforts. In addition, we call on government, using threat information and other intelligence, to increase law enforcement capabilities to disrupt, apprehend and prosecute cyber criminals.

- **CEO Commitments to Cybersecurity:** To support the objectives outlined above, the CEOs of Business Roundtable will invest in the infrastructure necessary to receive shared threat information and will develop the capabilities required to integrate cybersecurity threat and risk information into CEO risk management. We also recommend that boards of directors, as part of their risk oversight functions, continue to periodically review management's business resiliency plans, including cybersecurity, and oversee risk assessment and risk management processes, including those applicable to cybersecurity.

We are committed to working with Congress and the Administration to achieve solutions that provide the public and private sectors with the intelligence and tools necessary to collaboratively confront sophisticated cybersecurity risks.

I. Background

Cybersecurity threats from well-financed and motivated adversaries have the potential to disrupt critical services provided by private enterprise at home and abroad. Threats are increasingly targeting core functions of the government, economy and U.S. national security infrastructure, creating a shared risk to both the public and private sectors. Recognizing the seriousness of these threats, Business Roundtable member companies have made cybersecurity a top priority for more than a decade and have worked with their sector-specific government agencies to secure their networks and infrastructure.

Under Homeland Security Presidential Directive 7, the Department of Homeland Security (DHS) and designated federal agencies are required to identify, prioritize and protect U.S. critical infrastructure from terrorist attacks. In addition, the National Infrastructure Protection Plan (NIPP), updated in 2009, calls for greater information sharing about cybersecurity threats and urges risk-based adoption of protective measures. Roundtable companies have organized around this model, with many taking leadership roles on sector coordinating councils and operational information sharing centers, and have invested heavily in resources to share best practices and situational awareness (see Appendix A). In addition, companies have allocated significant resources to implement new sector-specific cybersecurity regulations established since 2001.

However, despite substantial public and private-sector investments, existing cybersecurity capabilities have not benefited from robust information sharing. As a result, public and private risk assessment and mitigation models have not evolved to the point where they can guide deployment of resources in the most valuable way. In such a dynamic cyber threat environment, without timely and actionable information about threats beyond those the private sector can typically identify and mitigate, companies must speculate as to the greatest risks and how to address them.

To keep pace with evolving cybersecurity threats, the public and private sectors must leverage and retool current legal and policy constructs. To date, members of Congress and the Administration have developed two different approaches to address cybersecurity risks to critical infrastructure:

- The first approach calls for the creation and adoption of cybersecurity practices to address risks. These proposals focus on the government creation of minimum security requirements for critical infrastructure and regulatory review and adoption of minimum security requirements. We are concerned that these proposals would shift the nation's resources toward a static, compliance-based regime to address cybersecurity threats over a more dynamic information sharing and risk management solution.

- The second approach calls for more robust information sharing on the specific threats faced by the public and private sectors. Notably, the House of Representatives passed H.R. 3523, the Cyber Intelligence Sharing and Protection Act (CISPA), in April 2012. The bill amends the National Security Act of 1947 to enable national intelligence agencies to share strategic threat assessments and other pertinent intelligence, including classified information, with private-sector entities that own or operate major information systems and other critical infrastructure systems. More important, the bill removes legal barriers to information sharing and establishes a protected framework for the bidirectional sharing of information between the public and private sectors. We consider legislation such as CISPA a positive first step toward establishing the real-time information sharing that is required for the public and private sectors to address cybersecurity risks.

While information sharing legislation is needed to set the course for cybersecurity preparedness, we also believe that once information sharing mechanisms are in place, additional action is required to ensure that information exchanged between the public and private sectors is effective and aids in the collaborative management of cybersecurity risks. Toward those ends, we have developed a proposal — detailed in the next section — that includes recommendations covering information sharing, threat-informed risk management and CEO involvement.

II. Proposal

The CEOs of the Business Roundtable are committed to maintaining and enhancing their ability to defend against cybersecurity threats and have developed a cross-sector solution to do so. Our proposal for a collaborative cybersecurity partnership between the public and private sectors calls for:

- **Information Sharing:** We support legislation that creates robust, two-way information sharing, with appropriate legal and privacy protections, between government and the private sector to exchange the specific threat information that will allow both government and business to better secure the nation's cyber assets and mitigate emerging threats in real time. The government must create a clear and concise legal framework for both private sector to private sector and private sector to public sector sharing, with appropriate liability, antitrust and freedom of information protections for those acting within the framework. All of the actions we propose depend on the advancement of information sharing and the removal of current legal barriers.

- **Threat-Informed Risk Management:** Once cyber threat information is readily shared between the public and private sectors, it will be necessary to expand existing efforts to develop threat-informed risk management and mitigation methodologies. To accomplish threat-informed risk management, new policies must build on existing sector coordinating councils and government operations centers and position senior public and private-sector leaders to collaboratively oversee cybersecurity efforts. In addition, we call on government, using threat information and other intelligence, to increase law enforcement capabilities to disrupt, apprehend and prosecute cyber criminals.

- **CEO Commitments to Cybersecurity:** To support the objectives outlined above, the CEOs of the Roundtable will invest in the infrastructure necessary to receive threat information and will develop the capabilities required to integrate cybersecurity threat and risk information into CEO risk management. We also recommend that boards of directors, as part of their risk oversight functions, continue to periodically review management's business resiliency plans, including cybersecurity, and oversee related risk assessment and risk management processes, including those applicable to cybersecurity.

To achieve the goals outlined above, we offer the following detailed recommendations. In addition, Appendix B of this report provides an overview of the specific government and Business Roundtable company commitments that will be required to achieve the goals outlined in our proposal.

Recommendations for More Intelligent, More Effective Cybersecurity Protection

1. **Threat Identification, Assessment and Law Enforcement:** Authorize and create two-way information sharing to actively exchange reports on imminent threats, response actions and situational awareness as well as deliver strategic threat assessments, such as National Intelligence Estimates, and increase law enforcement capabilities to disrupt, apprehend and prosecute cyber criminals.

2. **Risk Management and Mitigation:** Manage cybersecurity risks by building upon existing public-private partnership initiatives to develop threat-informed risk management and mitigation methodologies to address the most consequential risks to critical systems, assets and networks.

3. **Governance and Operations:** Position the public and private sectors to collaborate on cybersecurity at strategic and operational levels.

4. **Continuous Improvement:** Commit to focused research and development to continually improve cybersecurity capabilities as threats evolve — especially those functions supporting public-private information sharing.

5. **Accountability:** Invest in information sharing infrastructure and integrate actionable threat information into CEO risk management and board oversight activities to guide decisions and oversight related to strategic planning and budgeting, organizational structure and training, and internal control.

1. **Threat Identification, Assessment and Law Enforcement:** *Authorize and create two-way information sharing to actively exchange reports on imminent threats, response actions and situational awareness as well as deliver strategic threat assessments, such as National Intelligence Estimates, and increase law enforcement capabilities to disrupt, apprehend and prosecute cyber criminals.*

Lack of private-sector access to reliable threat information is the greatest impediment to effective cybersecurity protection of critical infrastructure. We propose the creation of a protected, real-time, two-way information sharing capability to ensure that public and private efforts to harden infrastructure and employ mitigations are guided by threat information.

Specific components required for effective information sharing include:

- **Implementation of Supporting Legal Frameworks and Protections:** Successful information sharing will require the development of an overarching framework that enables the open and honest exchange of cybersecurity threat information. This framework should include:

    - *Strong Liability Protections:* Legislation should include liability protections that remove the grounds for civil and criminal causes of action for companies that participate in information sharing and make good-faith decisions based on information that is obtained, identified or shared as part of information sharing activities.

    - *Protection of Privacy and Civil Liberties:* Legislation and policy should endeavor to establish appropriate protections of privacy and civil liberties, including requirements for information sharing activities to protect personally identifiable information.

    - *Policies and Protocols for Information Handling:* Legislation and policy should include flexible protocols to guide the exchange of company information provided to the government, including the "re-sharing" of company information beyond the intended recipient. Information sharing policies and protocols should be purposeful, action oriented and focused on operational improvements.

- *Penalties for the Release of Information:* Legislative solutions should include strong exemptions under the Freedom of Information Act and strengthened criminal penalties for the release of information.

- *Guidance on Antitrust:* The Administration should task the Department of Justice with issuing formal guidance on antitrust regulations to remove uncertainties and enable private-sector information sharing. Private-sector information sharing is of paramount importance to monitoring cybersecurity attacks that span sectors.

- **Increased Governmental Capabilities in Threat Identification, Assessment and Modeling:** The government must build its capabilities to provide the private sector with precise and actionable threat identification and assessment, including alerts on potential threats, proposed response actions, situational awareness and mitigation analysis. In addition, strategic threat assessments, such as National Intelligence Estimates, are required to inform owners and operators of pressing global cybersecurity threats.

- **Maximization of the Private Sector's Ability To Respond to Threat Information:** To promptly and effectively act upon threat information provided by the government, private-sector companies will have to work across their respective enterprises. As a result, the government must not only increase the number and level of security clearances within the private sector but also strive to share information that is classified at the lowest possible level to ensure that companies are able to share threat information with corporate stakeholders responsible for taking appropriate action.

- **Increased Focus on the Disruption, Apprehension and Prosecution of Cyber Criminals:** When the government shares information regarding active threats, private-sector companies must not only work operationally with the defense, civilian, intelligence and diplomatic components of the government to mitigate active threats but also be able to turn to law enforcement. As such, law enforcement must be fully resourced and equipped to apprehend cyber criminals. Prosecution of cyber criminals must be enabled by strengthened criminal penalties and sentencing. In addition, we encourage law enforcement to renew its focus on the development of capabilities to disrupt ongoing cyber attacks.

- **Enhanced Private-Sector Participation:** In return for government advancements in information sharing — especially in the area of liability protection — Roundtable companies are committed to providing the government with feedback on operational experiences associated with acting upon shared information, including the extent to which information provided by the government was timely and of an actionable nature, the effectiveness of any deployed mitigations, and the consequences if identified threats become reality.

- **Joint Development of Frameworks and Architectures for Information Sharing:** The public and private sectors should continue to work at the operational level, such as through the Critical Infrastructure Partnership Advisory Council, to jointly develop frameworks and architectures, including eligibility and minimum security requirements, to guide the development and implementation of information sharing infrastructure.

- **Adoption of Frameworks and Architectures:** Once frameworks and architectures are approved by the public and private sectors, sectors that are already regulated should adopt the frameworks and architectures into sector-specific law and policy. For those that are not regulated, sector coordinating councils should promote the frameworks and architectures within their sectors.

2. Risk Management and Mitigation: *Manage cybersecurity risks by building upon existing public-private partnership initiatives to develop threat-informed risk management and mitigation methodologies to address the most consequential risks to critical systems, assets and networks.*

Based on specific threat information shared by the government, companies and the government should invest in developing advanced and collaborative risk management and mitigation capabilities to keep pace with evolving threats. we propose that Congress and the Administration leverage current public and private investments in the NIPP risk management framework by directing:

- **Government Identification of the Most Severe Cybersecurity Threats:** All risk management activity should be predicated on precise and actionable threat information provided by the government to the private sector. Furthermore, the government should focus time and resources on identifying the highest risk threats that present the most severe consequences to each sector — such as those threats propagated by nation states and other well-resourced threat actors.

- **Sector-by-Sector Threat-Informed Risk Assessments:** Based on threat information provided by the government, Business Roundtable companies commit to working with sector-specific agencies to develop a process, where processes are not contained in existing regulation, for owners and operators to identify critical assets, systems and networks that could be targets of active threats and, subsequently, perform sector-level risk assessments.

- **Processes for the Negotiation of Technical Support:** Based on threat-informed risk assessments, the public and private sectors should collaborate on how to best deploy technical support from the government to address serious risks. Levels of support and other conditions should be considered in advance to work effectively when needed.

- **Deployment of Mitigation Strategies:** The private sector should collaborate by sector, and potentially across sectors, to deploy mitigation strategies based on the outcome of threat-informed risk assessments. Changes in the risk environment should be periodically monitored against threats, and risk assessments should be updated accordingly.

3. Governance and Operations: *Position the public and private sectors to collaborate on cybersecurity at strategic and operational levels.*

The nation's cybersecurity efforts should be supported by a renewed focus on strong public-private governance and operational capabilities. We support policies that:

- **Leverage an Existing Senior-Level Consortium To Oversee Cybersecurity Efforts:** We propose that Congress or the Administration task a consortium of senior leaders from the public and private sectors, such as the National Infrastructure Advisory Council or the National Security Telecommunications Advisory Committee, to perform governance functions and assess progress toward addressing cybersecurity risks by:

    - Making strategic recommendations to the President and sector agencies on the most pressing cybersecurity risks to the nation, based on informed threat and risk assessments;
    - Ensuring that resources dedicated to protect and mitigate against the greatest cybersecurity threats and vulnerabilities are allocated using cost-benefit analyses; and
    - Monitoring and reporting on the implementation, integration and effectiveness of cybersecurity capabilities recommended by the consortium.

- **Align Public and Private Operational Capabilities:** We propose leveraging and reinvigorating existing public and private-sector entities to implement the preceding components of the our proposal. Our companies have invested heavily in the development of best practices, the Critical Infrastructure Partnership Advisory Council, and Information Sharing and Analysis Centers (ISACs). The government has also invested in cybersecurity capabilities within the Department of Defense (DoD), DHS and other sector-specific agencies. These existing resources must be harnessed to support information sharing and risk management activities, such as the delivery of threat and risk assessments. Where appropriate, incentives should be considered to drive the further development of information sharing capabilities within ISACs and in conjunction with government operating centers. These existing operational capabilities within the public and private sectors should be leveraged by:

- Integrating the full resources of the government to provide unified cybersecurity risk identification, analysis, mitigation and modeling;
- Ensuring that the government provides critical infrastructure businesses with actionable risk information to inform corporate risk management;
- Executing recommendations made by the consortium; and
- Assisting in developing and implementing cybersecurity capabilities.

Realization of this goal will require rapid maturity of government capabilities. As such, we are committed to working with federal government partners, especially within DHS, to build governmental capability and expertise.

4. Continuous Improvement: *Commit to focused research and development to continuously improve cybersecurity capabilities as threats evolve — especially those functions supporting public-private information sharing.*

Current proposals identify discrete areas for capability development, but a unified public-private strategy is needed to optimize investments and leverage those institutions that are best positioned to advance key cybersecurity capabilities. We propose that the government realign research and development to focus on the following:

- **Real-Time Mitigation:** Using the information sharing framework contained in CISPA, invest in developing advanced monitoring and countermeasure capabilities with a goal of analyzing and mitigating cybersecurity risks in real time.
- **Advanced Risk Management and Modeling:** Employing the strategic threat-based risk management framework proposed herein, commit to developing a governmental capability to improve dynamic risk management and modeling. Developing this capability will require investment in a knowledgeable workforce able to perform such analysis as well as investment in supporting technologies and methodologies.
- **Effectiveness of Mitigation Strategies:** As the dissemination of threat information and risk management techniques advances, develop private-sector capability to examine how effectiveness can be measured, problem areas identified, and outcomes and improvements tracked.

- **Workforce Development:** Identify skills required to advance national cybersecurity goals and explore strategies within government, the private sector and academia to promote these skills.

- **Incentives for Cybersecurity Innovation:** As cybersecurity threats continue to evolve, continue to innovate to keep pace with adversaries. Legislation and policy should include a range of incentives to spur long-term innovation in cybersecurity.

5. Accountability: *Invest in information sharing infrastructure and integrate actionable threat information into CEO risk management and board oversight activities to guide decisions and oversight related to strategic planning and budgeting, organizational structure and training, and internal control.*

The development and implementation of information sharing infrastructure will require both investments and business process changes from private-sector companies. We commit to creating capacity and infrastructure within companies to accept national security threat information, including investments to gain security clearances for staff. In addition, we commit to ensuring that company information sharing infrastructure and processes are designed to share information with the government and other private-sector companies and organizations and to include experiences and impacts of preemptive actions and tactical responses to discovered threatening situations.

To incorporate actionable threat information into corporate functions, we are committed to:

- **Establishing and resourcing programs to incorporate cybersecurity threat information into company risk management by:**

    - Instilling the importance of cybersecurity in the culture of the corporation by setting tone and expectations;
    - Assigning responsibilities and developing appropriate metrics;
    - Actively monitoring and responding to ongoing risks; and
    - Working collaboratively with government on an ongoing basis to improve and advance cybersecurity resilience.

- **Addressing cybersecurity risks deemed significant by developing and periodically assessing:**
  - Risk management processes;
  - Strategic planning and budgeting;
  - Organizational design and training programs; and
  - Internal controls.
- **Communicating with the board of directors about significant cybersecurity risks and planned responses.**

We also recommend that boards of directors continue to oversee cybersecurity risks to corporations. As part of risk oversight functions, boards of directors should periodically review management's business resiliency plans, including cybersecurity. Through the audit committee, or another designated committee, the board should oversee the corporation's risk assessment and risk management processes, including those applicable to cybersecurity, and the designated committee should report regularly to the full board on the risks that it oversees.

III. Conclusion

An effective cybersecurity policy must recognize the vital role that robust, two-way information sharing plays in giving companies the insight necessary to mitigate these threats. Once companies have access to the information they need, developing more precise risk assessments and deploying resources more effectively become possible. Companies have been investing and will continue to invest heavily in enhancing our security postures and providing leadership within the sector-specific framework called for by national cybersecurity policy, and we are prepared to invest in the special expertise and resources to deal most effectively with serious cybersecurity risks over the long term.

Appendix A: Sector-by-Sector Cybersecurity Activity

The following table illustrates examples of private-sector commitments to cybersecurity and current efforts to defend critical networks and assets. This list is intended as a high-level sampling of sector-by-sector activity and, as such, does not include all cybersecurity activity and does not reflect every collaborative effort under way. Each sector addresses cybersecurity in particular ways relative to its mission. Many of the examples of activities detailed below have been driven by existing law and policy foundations — most notably Homeland Security Presidential Directive 7 and the NIPP as well as sector-specific law and policy. Current activity spans partnership and collaboration; risk assessment, management and mitigation; information sharing; best practices and standards; incident response; training, education and awareness; and research and development.

Cybersecurity Activity	Sector Activity
Partnership and Collaboration	◗ The **Chemical Sector** is actively engaged with DHS on implementing the "Roadmap to Secure Control Systems in the Chemical Sector." ◗ The **Communications Sector** is working cross-industry and with the government on a voluntary basis with more than 60 public-private initiatives. ◗ The investor-owned segment of the **Electric Sector** is engaged in the "Threat Scenario Project," an ongoing endeavor to identify threats, threat actors, mitigations and best practices to address cyber threats. ◗ The **Financial Services Sector** is actively engaged with the Cross-Sector Advanced Threat Task Force, addressing operational and strategic constructs with the federal government and various ISACs. ◗ The **Nuclear and Electric Sectors** are in the process of creating a working group that will include CEOs, White House national security staff, and Department of Energy (DOE) and DHS deputy secretaries to begin planning and preparing for response and recovery efforts before a disaster strikes. ◗ The **Nuclear Sector** Joint Cybersecurity Sub-Council serves as the focal point for Nuclear Sector participation in national efforts to deter, respond to and recover from cyber-attacks. ◗ The **Oil and Gas Sector** works closely with the **Chemical Sector** to ensure communication of inter-related standards, training, education, research and development, and best practices through associations such as the American Petroleum Institute, American Chemistry Council, and American Fuel & Petrochemical Manufacturers. ◗ The **Postal and Shipping Sector** and the **Transportation Systems Sector** work collaboratively on the Transportation Systems Sector Cyber Working Group, which coordinates and assists cybersecurity development for transportation elements.

Cybersecurity Activity	Sector Activity
Risk Assessment, Management and Mitigation	◗ The **Chemical Sector** is regulated by DHS under the Chemical Facility Anti-Terrorism Standards, which require high-risk chemical facilities to conduct cybersecurity risk assessments and implement mitigation measures that meet stringent federal standards. ◗ The **Chemical Sector** is working with DHS on the CARMA Risk Assessment Methodology, which provides a sector assessment of cybersecurity risks. ◗ The **Chemical Sector's** American Chemistry Council requires that all of its members implement the Responsible Care® Security Code, which requires cybersecurity risk assessment, management and mitigation and is audited by a third party. ◗ The **Communications Sector** Coordinating Council is conducting Communications Sector risk assessments that identify critical assets and specific threats to those assets. ◗ The **Dams Sector** published a "Roadmap to Secure Control Systems" to provide a comprehensive framework and recommended strategies to enhance the sector's understanding and management of cyber risks, facilitate the identification of practical risk mitigation solutions, and improve sectorwide awareness of cybersecurity concerns. ◗ The **Financial Services Sector** is engaged with the "Mythbusters Sharing Mechanism Systemic Risk Assessment Process" to improve coordination in response to significant events that pose risks. ◗ The **Information Technology Sector** worked with the International Organization for Standardization to issue ISO 27005 covering risk management approaches for information security. ◗ The **Oil and Gas Sector's** Project LOGIIC is partnering with DHS to improve process and operational technology for cybersecurity. ◗ The **Water Sector** Coordinating Council has developed the "Roadmap to a Secure & Resilient Water Sector" and the "Roadmap to Secure Control Systems in the Water Sector." Both act as a unified security strategy containing specific goals, milestones and activities to mitigate cybersecurity risks.

Cybersecurity Activity	Sector Activity
Information Sharing	◗ The **Chemical Sector's** American Chemistry Council maintains a Cyber Incident Response Program that provides members a protected environment for sharing information during a major cyber incident. ◗ The **Chemical Sector's** American Chemistry Council ChemITC organization provides members regular forums to share best cybersecurity practices. ◗ **Chemical Sector** cybersecurity experts joined with cybersecurity leaders in the **Oil and Gas** and **Water Sectors** to develop industrial control system security standards. Chemical Sector guidance documents were used to jump-start the standards development work. ◗ The **Chemical Sector** has developed and is using benchmarking surveys to assess and measure progress toward achieving cybersecurity improvement goals. ◗ The **Communications Sector** ISAC's mission is to facilitate voluntary collaboration and information sharing among government and industry with the goal of averting or mitigating impact upon the telecommunications infrastructure. ◗ The **Defense Industrial Base (DIB)** participated in a voluntary cybersecurity information sharing pilot between the DoD, DHS and eligible DIB companies. ◗ The **Financial Services** ISAC receives timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cybersecurity threats. ◗ The **Information Technology** ISAC collaborates with other sector-specific ISACs and assists them in understanding cybersecurity threats. ◗ The **Critical Manufacturing Sector** Information Sharing Working Group serves as a joint working group that addresses information sharing issues of concern to the sector, including information sharing policy and practices with regard to communication, collaboration and coordination, and operational awareness. ◗ The **Oil and Gas Sector,** through the American Petroleum Institute Technology Committees and Subcommittees, is sharing cybersecurity information regarding risk assessments, incidents, threats, protection and mitigation in quarterly meetings and during the annual American Petroleum Institute Cyber Security Conference as well as on an ongoing basis.

Cybersecurity Activity	Sector Activity
Best Practices and Standards	◗ The American Chemistry Council's ChemITC organization provides members of the **Chemical Sector** regular opportunities throughout the year to share best cybersecurity practices, which culminate each year in the ChemITC Annual Conference. ◗ Since 2003, members of the **Chemical Sector** have worked together and published several cybersecurity awareness and best practice guidance documents under CIDX® and later the American Chemistry Council. ◗ The **Chemical Sector** maintains a website on the "Roadmap to Secure Control Systems in the Chemical Sector," which acts as a clearinghouse for information, standards and best practices (www.chemicalcybersecurity.com). ◗ Cybersecurity guidance was adopted and included within the **Chemical Sector's** American Chemistry Council Responsible Care Security Code. ◗ The **Communications Sector** participates in the Federal Communications Commission — Communications Security, Reliability and Interoperability Council and has created ISP network protection best practices and cybersecurity best practices. ◗ The **Financial Services** ISAC's Account Takeover Task Force creates best practices for fraud prevention, detection and customer awareness for online financial institutions. ◗ The **Electric Sector** has recently passed version five of the Critical Infrastructure Protection Standards, which further identify critical assets and include standardized measures to create a strong baseline level of security through the North American Electric Reliability Corporation. ◗ The **Electric Sector** is participating in a joint effort led by DOE and DHS, the Cybersecurity Capability Maturity Model, to assess cybersecurity readiness. ◗ The **Health Care and Public Health Sector** has established the health information exchange (HIE) standards and security controls for the exchange of protected health information, as defined under the Health Insurance Portability and Accountability Act, and developed a methodology to support the security architecture design of HIEs and health information networks. ◗ The **Information Technology Sector** is using internationally developed and accepted standards, such as the ISO 27000 standards, to improve cybersecurity. ◗ The **Oil and Gas Sector's** American Petroleum Institute best practices and standards as well as international standards are used to protect network and operational technology systems from cyber threats.

Cybersecurity Activity	Sector Activity
Incident Response	◗ The **Chemical Sector** has been an active participant in the DHS Cyber Storm exercises that test the sector's ability to respond during a crisis. ◗ The **Chemical Sector's** American Chemistry Council maintains an emergency alert system for its members to use during a significant cybersecurity event to create situational awareness. ◗ The **Chemical Sector** has implemented a Cyber Incident Response Plan to quickly engage cybersecurity leads at chemical facilities to communicate risks and appropriate response actions. The system is invoked through the CHEMTREC Emergency Service. ◗ The **Financial Sector** is working on a private, sectorwide Cyber Incident Response Plan for major events in cyberspace that threaten the sector. ◗ The **Oil and Gas Sector** is working with DOE to rapidly respond to cybersecurity incidents under the NIPP.
Training, Education and Awareness	◗ Each year, the American Chemistry Council's ChemITC organization puts on the ChemITC Annual Conference, which is aimed at sharing best cybersecurity practices and elevating awareness in the **Chemical Sector.** ◗ In conjunction with DHS, **Chemical Sector** industrial control system security experts have assembled the "Roadmap to Secure Control Systems in the Chemical Sector" document, other security guidance documents, training opportunity listings, business cases for adopting cybersecurity practices and other reference materials and published these on CDs for distribution at industry conferences and trade shows. ◗ The **Financial Services Sector** has been engaged with the National Cyber-Forensics and Training Alliance to educate and work through scenarios related to identifying and mitigating cybersecurity threats that target the sector. ◗ The **Oil and Gas Sector** conducts frequent cybersecurity workshops and conferences through the American Petroleum Institute, American Fuel & Petrochemical Manufacturers, American Gas Association, and Interstate Natural Gas Association of America to foster a greater awareness of cyber threats to sector networks and operating systems. ◗ The **Transportation Systems Sector's** owners and operators have built a strong training and education foundation that includes a wide range of programs to effectively secure transportation assets, systems and networks.
Research and Development	◗ The **Financial Services Sector** is engaged with the Advanced Cyber Security Center to develop a collaborative, cross-sector research environment to address the most critical and sophisticated cybersecurity challenges.

Appendix B: Proposal — Summary of Government and Company Commitments

To further detail the specific commitments contained in the "Proposal" section of this report, the following table delineates government and Business Roundtable company commitments that will be requited to achieve the goals of our proposals, by recommendation area.

Government Commitments	Business Roundtable Company Commitments
1. Threat Identification, Assessment and Law Enforcement	
◗ Deliver strategic threat assessments and real-time operational threat information on active cyber threats, implement supporting legal frameworks and protections, and develop the capacity to enable both operational and law enforcement responses. ◗ Increase law enforcement capability to disrupt, apprehend and prosecute cyber criminals.	◗ Participate in the exchange of information on threats, including providing private-sector information and mitigations, and assist the government in refining information sharing capabilities.
2. Risk Management and Mitigation	
◗ Build on existing foundations to develop threat-informed collaborative risk management, modeling and mitigation methodologies and techniques to enable sector risk assessments.	◗ In collaboration with sector-specific agencies, perform threat-informed sector risk assessments and deploy mitigations to address risks.
3. Governance and Operations	
◗ Mature governance and operations supporting cybersecurity: • Leverage an existing public-private consortium, such as the National Infrastructure Advisory Council or National Security Telecommunications Advisory Committee, to make recommendations on how to improve the nation's cybersecurity posture; and • Integrate governmental cybersecurity functions across defense, homeland security, intelligence, law enforcement and diplomatic components.	◗ Participate as an equal partner in cybersecurity: • Contribute senior leadership to consortium; • Continue investments in operational centers (e.g., ISACs); and • Align operational centers with government integration efforts.
4. Continuous Improvement	
◗ Continually improve vital cybersecurity capabilities: • Advance information sharing environments by committing to research and development in the areas of real-time mitigation and analysis, as well as risk management and modeling; • Work with companies to build skill sets in the cybersecurity workforce; and • Provide incentives to encourage cybersecurity innovation over the long term.	◗ Work with the government as well as within and across sectors to continually improve vital cybersecurity capabilities: • Partner with the government to enhance information sharing environments; • Gauge the effectiveness of mitigation strategies; and • Build workforce knowledge and capacity.

Government Commitments	Business Roundtable Company Commitments
5. Accountability	
◗ None, this section is specific to Business Roundtable companies.	CEOs commit to: ◗ Establish and resource programs to incorporate cybersecurity threat information into company risk management by: • Instilling the importance of cybersecurity in the culture of the corporation by setting tone and expectations; • Assigning responsibilities and developing appropriate metrics; • Actively monitoring and responding to ongoing risks; and • Working collaboratively with government on an ongoing basis to improve and advance cybersecurity resilience. ◗ Address cybersecurity risks deemed significant by developing and periodically assessing: • Risk management processes; • Strategic planning and budgeting; • Organizational design and training programs; and • Internal controls. ◗ Communicate with the board of directors about significant cybersecurity risks and planned responses. Recommendations for Boards of Directors: ◗ As part of the board risk oversight function, periodically review management's business resiliency plans, including cybersecurity. ◗ Through the audit committee, or another designated committee, oversee the corporation's risk assessment and risk management processes, including those applicable to cybersecurity, and report regularly to the full board on the risks that it oversees.

300 New Jersey Avenue, NW
Suite 800
Washington, DC 20001

Telephone 202.872.1260
Facsimile 202.466.3509
Website brt.org

Printed on recycled paper