FORCEPOINT
POWERED BY Raytheon

Response for

The Department of Commerce (DOC) - National Institute of Standards and Technology (NIST)

REQUEST FOR INFORMATION

Property	Description
Customer and Contact	National Institute of Standards and Technology Nakia Grayson, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Email Address: *cybercommission@nist.gov*
Document Name	Request for Information:
Document Owner	Forcepoint™ 12950 Worldgate Dr. Suite 600 Herndon, VA
Document Author and Contact Information	Stacey Winn Sr. Manager, Federal Product Marketing Mobile: (703) 537-4356 Email: swinn@forcepoint.com
Creation Date	September 9, 2016

Forcepoint Disclaimer:

Forcepoint has prepared the content in this document ("Proposal") solely for the National Institute of Standards and Technology in response to the RFI. This Proposal is the result of Forcepoint's good-faith efforts, however its content is not comprehensive nor has it been independently verified. The information provided in this Proposal is the confidential and proprietary intellectual property of Forcepoint and any contributing party to the Proposal, and no right is granted or transferred in relation to any intellectual property contained in this Proposal. No part of this Proposal may be communicated to any other party without the prior written approval of Forcepoint. This Proposal is provided AS IS, and Forcepoint makes no representation or warranty, express or implied, including without limitation the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. In no event will Forcepoint be liable for any direct, indirect, incidental, consequential, special, or punitive damages related to this Proposal. No legally binding contract relating to the Forcepoint products and solutions referred to in this Proposal exists or will exist until such time as a mutually agreed upon definitive agreement providing for the use of Forcepoint's products has been formalized. By accepting this Proposal and the information therein, the recipient agrees to the foregoing.

Ms. Nakia Grayson
Email Address: cybercommission@nist.gov

September 9, 2016

Dear Ms. Nakia Grayson,

Forcepoint™ (Powered by Raytheon) is a joint venture of the Raytheon Company and Vista Equity Partners. Forcepoint operates as an entirely separate company, with financials being reported by Raytheon. Forcepoint is built on the successful integration of Raytheon Cyber Products, Websense and the acquired Stonesoft next-generation firewall business. The combination of these organizations brings together decades of front-line experience across many domains of cybersecurity, from Fortune 100 enterprise to mid-sized businesses in every industry, to the world's most highly secure defense, civilian, intelligence and law enforcement agencies.

The following proposal was created in response to the requirements stated in your RFI. We look forward to having further face-to-face discussions with you and your team and demonstrating how Forcepoint can meet your requirements as you move on to the next phase of your project. Please feel free to contact me at (703) 537-4356 or at swinn@forcepoint.com should you require any additional information.

Sincerely,

Stacey Winn

Sr. Manager, Forcepoint Federal Marketing

Institute for Critical Infrastructure Technology (ICIT) Fellow

Contents

Executive Summary

Forcepoint™ is pleased to respond to the Request for Information (RFI) for the National Institute of Standards and Technology (NIST) to assist the Commission on Enhancing National Cybersecurity in the definition of technology and solutions needed to best address current and future states of cybersecurity in the digital economy.

Government and commercial entities are constantly on alert to prevent and fight against the ongoing threat of cyber-attacks. The dichotomy faced by today's enterprises is that in order to protect themselves against these threats they must also collaborate and share information across sensitivity levels within their own organizations and also across government and corporate boundaries. In light of this, network security is of paramount significance especially with the keen emphasis currently placed on secure collaboration and information sharing in an environment of increasing threats and vulnerabilities.

Forcepoint safeguards users, data and networks against the most determined adversaries, from accidental or malicious insider threats to outside attackers, across the entire threat lifecycle. Forcepoint protects data everywhere – in the cloud, on the road, in the office – simplifying compliance and enabling better decision-making and more efficient remediation. Forcepoint empowers organizations to concentrate on what's most important to them while automating routine security tasks. More than 22,000 organizations around the world rely on Forcepoint.

Forcepoint products are well suited for implementation in any network and are able to address many network security and boundary protection challenges. The product suite includes multi-level access solutions designed to reduce hardware footprint while allowing secure, simultaneous access to multiple networks of varied classification levels from a single workstation, cross domain transfer solutions to automate and audit secure data movement between networks, content protection solutions to protect sensitive data across the enterprise, and advanced analytics to allow virtual data warehousing for federated searches and behavioral analysis.

For this RFI, we have focused on providing comments and inputs related on the Topic Area **Critical Infrastructure Cybersecurity** while addressing the questions presented in the RFI.

Addressing Key Points in the RFI

Critical Infrastructure Cybersecurity

Our critical infrastructure and the energy sector specifically have a complicated balance between business efficiencies, cybersecurity and national security. As is well known in the energy sector, if a portion of the grid goes down the impact across all economic, national and even international sectors can be impacted. While it is complicated – it is also a recognized need where many best-practices from other industries including the Public Sector can be applied. Recognition of the problem and having discussions, awareness and avenues such as the Institute for Critical Infrastructure Technology (ICIT) to foster the dialogue between concerned parties is a productive path forward to establishing future standards.

Some of the challenges we all face as Security Professionals and especially within the Critical Infrastructure environment are:

- New technologies entering the marketplace at a rapid pace. With today's "always on, always connected" world of cloud, mobile and Internet of Things we must **adopt transformative technologies** and the innovation they bring. But we must also consistently apply and adapt security principles and techniques even as we realize productivity and cost savings benefits from moving data to clouds and rely on remote administration capabilities.

- All of this interconnection provides many benefits –namely cost savings and productivity. With those benefits comes the need to **combat escalating threats**. It is not if a breach will occur but when – when all your networks and devices are connected the risk to your entire enterprise is much greater when that breach does occur

- In this frame you also have a plethora of vendors talking about much the same thing - what are you ultimately looking to achieve? **Better risk management** to lower the impact of a breach and the ability to demonstrate resiliency and get back to business.

Keeping these challenges in mind, the current threat state consists of:

- **Flat, interconnected network topologies** that can allow adversaries unrestricted access to move laterally from one server to another increasing the dwell time, or length of time resident in the network.

- **Changing Perimeters**: **Mobile/BYOD/Cloud**. No longer do employees come to one office every day and log in to a tower CPU. Now employees work from wherever they are – they use multiple devices – sometimes even their personal devices – and they access clouds be they public, private, on or off premises, or some combination.

- **3rd Party Credential Compromise:** One of the many things that the high-profile breaches show us is that it isn't just our organizations' security we have to be concerned with but also the security practices of our 3rd party contractors and supply chain companies and their levels of access.

- **IoT: Promise & Vulnerability:** Internet of Things brings even more connections promising to make our lives easier; however, the ease of use and access that can be gained are tempered with the high degree of risk for compromise of potentially sensitive information, increasing risk and vulnerability

Data Sharing

The U.S. Department of Defense, Intelligence Community, and Civilian government agencies rely on physical network separation to mitigate risk and protect sensitive and classified environments. This network structure is very secure but it is often cumbersome to work in and administer: multiple desktop machines for each end-user, difficulty in ensuring the right data is accessible to the right end-users in the right locations, and the time and expense of managing many software images. Multi-level Security (MLS) Cross Domain technologies can be used to securely and easily Access and Transfer data and information between and within these physically separated networks.

Secure information sharing of critical data is key to increase business efficiencies. While this has been a huge benefit to organizations in managing their businesses it has also become a huge vulnerability. One example is when Operations Technology (OT) systems – that tend to be legacy systems and not always maintained to the same standards as Information Technology (IT) systems – are connected directly or indirectly to systems with broader user bases and access to the open Internet.

While an air gap between these systems for network isolation is a good start – additional security measures are also required that will enhance the security posture but also allow the right data to securely move where it needs to. Any sophisticated network isolation solution – such as those used within the Department of Defense – should include **multiple layers of defense** to provide redundancy and additional monitoring of data flows.

Beyond just unique configuration, internal data separation, mandatory access controls, restrictions on administrator actions and strict configuration integrity assertions, multi-level secure data transfer technology also makes extensive use of customized software to perform all transfers, greatly reducing the risk of the common attack vectors.

Securing an Interconnected World: Leveraging Segmented Networks

Physical segregation of internal and external networks to reduce the attack surface, combined with secure operating systems and secure multi-level access and transfer solutions for usability, is a fundamental element for critical infrastructure protection. For example, segregating the SCADA network from the corporate LAN (switch and firewall are no longer connecting to SCADA LAN). The SCADA LAN can be further segregated from the field device network (RTUs, PLCs, IEDs, etc.), by establishing an electronic security perimeter (ESP).

What can we do to both leverage these innovative and necessary technologies while also managing risk and ensuring organizational and personal security? **Network Segmentation** is one such technique.

- **Move away from flat, interconnected networks** – instead – identify where your most sensitive networks reside and use that as a guide to physically separate networks from each other with the goal of putting your most critical network as far inside as possible and away from less restrictive access points.

- Employ **virtualization** and **secure redisplay** technologies to move desktops and data to a central datacenter or cloud

- Enable users secure access to **only allowed networks** from a single endpoint device **through cross domain multi-level solutions** that also provide streamlined administration

With this design and philosophy – **Network Segmentation** becomes a security best practice.

Throughout Department of Defense, Intelligence Community and within the Federal sector, security teams are charged with protecting our most critical data and assets. Networks are physically separated, housed in secure datacenters and access levels are strictly followed. How does this apply to the **private sector**?

Most organizations can benefit from this security best practice, bringing defense-grade protection to commercial entities like Critical Infrastructure and Financial Services. Keep sensitive data and networks isolated and protected – not public-facing.

The proliferation of new data sources promises to compound security challenges. Organizations must embrace a new way to protect their valued assets and information, building robust assurances against data leaks, spills and theft as well as any compromise of data integrity. Cross domain solutions offer protection at the highest levels, and they facilitate secure collaboration at significantly lower costs than other methods.

The defense and intelligence industries are at the forefront of this initiative to better secure information. They must continue to stay the course. With threats escalating in complexity and severity, it is only a matter of time before their civilian counterparts and commercial industry follow suit. This need has been building over time.

As computers started to multiply, manufacturers did not perceive security as a primary driver in the process. They proceeded to store everything on flat networks and continue to do so chiefly out of consideration for cost and ease of management. The Defense Department and the intelligence community, on the other hand, went through the pain of classifications and the compartmentalization of information and assets across separate physical domains. In many ways, this move benefited both groups by minimizing data compromise and leakage better than their commercial counterparts. As threats become more serious, network segmentation and data classification will emerge as the next frontiers to ensure a higher level of defense and information assurance.

High-profile attacks reported on so far primarily have targeted commercial industries. One of the most highly publicized was the Target breach, wherein hackers stole customer data by compromising an HVAC vendor in the retailer's supply chain. In the government, the U.S. Office of Personnel Management (OPM) breach stands out as the watershed moment, affecting more than 21 million personnel records, including fingerprints. While each of the

organizations breached had mature security measures in place, a quick analysis presents an interesting discovery: All their networks were flat. Once inside a network, an adversary could move laterally and freely to attack critical servers.

If any of these organizations had segmented their networks and compartmentalized their data, there could have been a different story. At the very least, the adversary's job would have been much harder, and security teams might have found the compromise before it was too late. The fundamental concepts of data compartmentalization and network segmentation make sensitive data difficult to reach for adversaries but easy to access for authorized users. Data does not leak, spill or otherwise fall into the wrong hands inadvertently.

As the threat landscape changes, two additional alarming trends loom. One is the rise of insiders—either maliciously or accidentally—exfiltrating information. The other is the penchant for attackers to move away from data theft and toward compromise in favor of more menacing goals.

Yet just because networks are segmented and data is classified and compartmentalized does not mean the adversary will not try to attack. Therefore, it is important to apply segmentation across agencies. This can grow complicated quickly because agency and program requirements evolve constantly, and network segmentation should serve as a fundamental design, not as an afterthought. In many cases, a physical infrastructure, rather than just software, must be taken into account. Also, classified data generally cannot reside on the same domain or network as other data.

While segmentation can offer greater information assurance, it also can create budget burdens. If an agency opts for multiple domains, each application and physical hardware might have to be replicated for adequate service across these domains. An agency with 500 users who require three networks with email and print capabilities would mandate an email client be available to staffers on each network. This could bring the number of email clients up to 1,500. A printer for every 10 individuals would entail 50 printers at each user level and 150 across the three networks. In addition, if the agency has not acquired what are now considered readily available cross domain access technologies, each employee would need three client workstations, along with all the connectivity and power to go with them.

Classified data and segmented networks introduce a new challenge as well. Many objectives or functions feed on information from various places. Security standards do not easily allow co-mingled data. User rights must be considered down to a granular level. Access to information and applications and the safe transfer of data between domains represent two major concerns. In the former case, information and applications are not required to be physically moved. The latter dictates duplication.

While physically separating data establishes a greater degree of information assurance and confidence, the data still has to transfer across domains as needed for collaboration. Typically, an employee at a lower domain could seek a document or multimedia content from a higher domain to meet his or her objectives or to perform a function. But consider a soldier who usually does not have access to a classified domain who must listen to a broadcast from an officer residing at the more sensitive level. Instead of providing authorization to the higher domain, it may be better to stream the broadcast to users at the lower domain.

These examples illustrate the demand for technologies that not only help reduce costs but also enhance the secure

transfer of information on a need-to-share basis between user levels. In some cases, a physical transfer might be necessary; in others, duplication of data at additional levels is prohibited. Cross domain technologies are built specifically to address some of these difficult issues, leading to collaboration and secure access and transfer.

Firewall technology is ubiquitous, and it plays a key role. Although firewalls originally were devised to control access to private or enterprise networks from the outside, their latest incarnations offer more eclectic flavors. The basic kinds deliver some packet-filtering capabilities to ensure that only whitelisted sources are allowed through, but application firewalls or proxy servers bring more sophistication. They can intercept packets and forward them to specific applications inside an organization. Next-generation firewalls establish an integrated platform that combines basic firewall functionality with deep packet inspection, intrusion prevention, SSL and SSH interception, website filtering and anti-virus inspection.

The concept of guard technology, or cross domain multi-level transfer, has been around for a long time. Guards are similar to firewalls—both are border-protection devices that control entry to assets stored within the enclaves they defend. But they differ from firewalls in that, while the latter allows any traffic through and is configured to block unwanted traffic, guards operate on a zero-trust model, denying all sources access unless configured otherwise. Because their applications traditionally run in a high-risk and high-assurance environment, guards display a greater standard of confidence, evaluation and filtering functionality than firewalls.

Whether to apply a next-generation firewall or a guard depends on an organization's asset protection and assurance needs. The sensitivity of information transferred, the application sought, source and destination assurance levels and a host of additional issues dictate which choice is appropriate.

One example is a utility in the critical infrastructure industry. If a user is trying to access a supervisory control and data acquisition (SCADA) control from a different network, a guard would apply because an elevated degree of assurance is necessary. If status data generated from a controller in a substation is being transmitted to a central SCADA control, a firewall may be the appropriate choice if the substation controller is fairly isolated from untrustworthy networks.

While firewalls and guards control and audit information transfer, not all data has to leave its location to be accessed by a user. With transfer mechanisms, information physically moves from one location to another—either from a place of higher trust to one of lower trust, or vice versa. When data moves, essentially a copy is made. It is up to the custodians of the domain to establish appropriate protection. End users who access this information and store it on an endpoint frequently degrade information assurance. One reason is that smartphones and tablets used as part of bring your own device (BYOD) programs, which often receive overt or tacit approval from employers, are more prone to loss and theft. The upshot is that information assurance is less of a certainty than ever. In many circumstances, organizations should store data in appropriate enclaves. Authorized employees can use that data as necessary without physically transferring it to a second location.

In such cases, access to the various domains can be virtualized. The applications and data physically reside at the sensitivity levels to which they are assigned in a virtualized environment. Users access them through a secure redisplay mechanism. If users require availability from multiple domains, this can be facilitated through secure technologies that keep the separation of the physical enclaves all the way to the endpoint but introduce multiple

redisplay windows from which a user can retrieve the information.

In the government, one example of a complex environment requiring robust information security is the Department of Veterans Affairs. The health care ecosystem is defined by an intricate web of providers, patients, payers, pharmaceuticals, suppliers and more. As a result, the department handles a variety of sensitive information, including patient histories, billing details, credit card accounts and medical device data, and it must comply with myriad regulations. In most cases, information does not require transfer to a second location—to do so would degrade the nature of security around it. Should secure access and redisplay technologies be used in this type of environment, users still leverage apps and data that benefit the business and its mission. But the apps and data will not move physically or replicate to enable this flexibility.

In this type of construct, information assurance can generate savings, and agencies and organizations are looking for new ways to lower costs while augmenting security. In the United States, President Barack Obama's fiscal year 2013 budget called for cuts in unnecessary spending, including printing and supplies. This is understandable when studies show that organizations can cut their total printing budget by 65 percent through printer consolidation. Consolidation saves not only in hardware expenses but also in consumables and administration. When extraneous printers at multiple sensitivity levels are eliminated, organizations reap significant savings from reduced hardware, space, power, support and supplies. The robust defense provided by guard-based systems enables users to print safely to high-side printers from multiple security levels without the risk of transferring malicious or sensitive data from high-trust to low-trust networks.

Guard-based systems also enable the secure, policy-enforced exchange of email and attachments among users on different networks, designating a single inbox for all email activity. A single inbox boosts productivity for those who require access to multiple email clients residing on different networks at varying classification levels. This effort also cuts down on the number of email clients deployed across various domains, adding to budget savings.

Ultimately, agencies can reach a state of optimized protection through analysis. Yet whether it is analysis of environmental data, operational information or security data, analysts face the challenge of deploying tools at each clearance level and then correlating them across domains. This is a tedious task. With cross domain technologies, analysis tools are deployed at the high side, with protected data shared from other levels to foster a holistic view of information that drives easier analysis and lowers costs.

In multiple clearance-level environments in which analysts and users operate within various domains, endpoints must distinguish themselves to achieve separation. Depending on the number of domains involved, an analyst could end up with seven or eight workstations, creating onerous conditions and a space overwhelmed with heat. Cross domain technologies avoid this by providing users with secure, simultaneous access to information on any number of networks from a single thin client, cutting expenses and eliminating environment degradation.

Cloud technologies unveil a new paradigm for network segmentation as well, enhancing cost savings. Applications can reside on one level—such as the high side—and information associated with the applications can exist at other levels. Cross domain access to data would ensure that a user does not require multiple instantiations of an application but is allowed access to data from appropriate levels. Guards and next-generation firewalls also facilitate safe and secure transfer of information between multiple clouds, incorporating physical separation while offering a

higher level of assurance.

Insider Threat

Mitigating the cyber insider threat to include privileged users and credential management is important to establishing robust security measure for Critical Infrastructure.

The **2016 Ponemon Institute Study** on the Insecurity of Privileged Users found**:**

- **Increasingly, malicious insiders target privileged users to obtain their access rights.** In 2011, only 21% said it would be likely that malicious insiders would use social engineering – **such as spear phishing as** discussed in the recent ICIT publication "The Energy Sector Hacker Report: Profiling the Hacker Groups that Threaten our Nation's Energy Sector**"** – or other measures to obtain someone's access rights. This has **increased significantly to 46% of respondents**. In addition, more respondents say it is likely that social engineers outside the organization target privileged users to obtain their access rights (48%in 2016 and 30% in 2011).

- **Lack of visibility continues to hinder the ability to determine if users are complying with policies**. 39% of respondents are not confident that they have the enterprise-wide visibility for privileged user access and can determine if users are compliant with policies. Only 18 percent are very confident that they have this visibility.

- **To detect privileged user abuse, some organizations correlate activity from multiple sources.** 57% percent of respondents say their organizations do not have the capabilities to effectively monitor privileged user activities. However, 42% of organizations represented in this study are correlating activity from multiple sources such as trouble tickets and badge records to determine risky privileged user behavior. A lack of resources, in-house expertise and technologies are preventing companies from using correlation of trouble tickets and badge records to minimize the privileged user risk.

Solutions that enable the safe and effective use of business and mission-critical technologies by capturing technically observable human behaviors which include policy violations, compliance incidents or malicious acts that may be warning signs of an impending breach, can provide all the details, insight, and complete context (through video replay) to immediately assess the severity of the threat, remediate the problem, and build the policies to prevent it from happening in the future.

Summary

Implementing information sharing technologies for accessing and/or transferring sensitive data and insider threat/user activity monitoring tools are critical to protecting our nation's infrastructure from compromise no matter if there was actual malicious intent or an innocent act by an off-site employee. Forcepoint's solutions were developed for use by the Department of Defense (DoD) and the Intelligence Community (IC) and have been in operational use, worldwide, for over 20 years. The need for this robust technology has expanded to other federal and civilian agencies, law enforcement, first responders, and state and local officials as the need for sharing and protecting sensitive data has become paramount to protecting our communities and citizens.