STATEMENT

OF

JOHN B. WOOD

CHIEF EXECUTIVE OFFICER & CHAIRMAN

TELOS CORPORATION

HOUSE SCIENCE, SPACE & TECHNOLOGY SUBCOMMITTEES

ON

RESEARCH & TECHNOLOGY AND OVERSIGHT

HEARING ON

"CYBER SECURITY: WHAT THE FEDERAL GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR"

JANUARY 8, 2016

Chairman Smith, Ranking Member Johnson, Chairwoman Comstock, Ranking Member Lipinski, Chairman Loudermilk, Ranking Member Beyer, members of the Committee. My name is John Wood. I am CEO and Chairman of the Board of Telos Corporation, a cyber security company headquartered in Ashburn, Virginia.

Telos Corporation empowers and protects the world's most security-conscious enterprises with solutions and services for continuous security assurance of individuals, systems, and information. Our offerings include cyber security solutions and services for IT risk management and information security; secure mobility to protect globally connected enterprises; and identity management to establish trust in personnel and continuously monitor for insider threats. We serve customers in the military, intelligence and civilian agencies of the federal government, allied nations, and commercial organizations around the world.

I have been with Telos for 23 years, including serving the past 20 years as CEO. Twenty years is a long time in any business but in the rapidly changing world of cyber security, it often seems more like a hundred years.

I appreciate the invitation to discuss industry best practices from Telos' perspective, and to share with you my observations regarding how those private sector practices can and should be applied to the public sector. As a cyber security company and as a contractor that does a significant amount of work with military, intelligence and civilian agency customers, this is obviously a topic of great importance to Telos.

Last summer's disclosure of the massive OPM breach, on which you and other committees held hearings, highlighted for me an important lesson for executives in both the public and private sectors. That is, in every organization, whether it is a commercial entity or a government agency, the command chain needs to be intimately aware of cyber security issues; this means risk management needs to be overseen at the highest level. It has to be that way and it is irresponsible if such oversight is not happening. Senior management must receive frequent reviews and reports of the organization's cyber vulnerabilities, along with plans for remediation. Issues of cyber risk management and information security can no longer be solely shouldered by an organization's chief information security officer (CISO). Top executives must have a basic knowledge of their organization's cyber risk and take responsibility for the solution.

This also highlights the stated purpose of this hearing: what can the public sector learn from the private sector? In addition to having strong leadership at the top on cyber security issues, there has to be a commitment to a culture of cyber hygiene at the top that permeates through the entire organization. That's what we do, that's what many of our peers do, and that's what government agencies must do as well.

It is the responsibility of management to ensure that basic cyber security training is provided throughout an organization. This is borne out by the **2015 Verizon Data Breach Investigations Report** (DBIR), which said that "the common denominator across the top four patterns [of security incidents] — accounting for nearly 90% of all incidents — is people." Let's be clear what this means — the Verizon study found that a majority of security incidents reported may have been avoided if employees had taken *basic* cyber security precautions, like implementing

stronger passwords and two-factor authentication, patching software, and knowing how to recognize the signs of a phishing attack. Having a more educated employee base doesn't mean an entity is impervious to being hacked, but it does *significantly* decrease the chances and frees up resources for defending against the more sophisticated attacks.

The basics of information security cannot be ignored in day-to-day operations. A few years ago, one of our security experts came up with five basic steps that organizations should be taking to better protect themselves from attacks. These **risk management practices** are things we do, and we believe all organizations – public and private – should be doing them as well.

The first has to do with the basic **passwords** people use, regardless of whether two-factor authentication is used. Is eight characters still a good idea? What about nine, 10, or 20 characters? We need to strike the right balance between usability and security. The problem is, if a user gets a 20-character password, odds are they will write it down at their work station, or worse yet, put it in a file called 'passwords.txt' in their home directory. So there needs to be a balance – users need to have passwords that are as long as they can possibly remember without having to write it down somewhere or leave it in a computer file that can be a gold mine for hackers.

There are several ways to create strong passwords. One way is to use pass-phrases, which are easier for users to remember. Another approach is to use the first letter of every word in a phrase or sentence (use upper and lower case letters and numbers and special characters to replace letters when possible). You need strong passwords for all your employees, and they need to be diligent about making sure the bad guys can't guess their passwords.

The second step is **security awareness training**. It may not always succeed, but security training can help reduce the probability and number of data breaches that are attributable to human error, as noted in the Verizon report. Employees must be trained to know that if something is wrong they should report it – even if something only *appears* to be wrong, they should report it. A security awareness program operates just like an anti-terrorism operation; it cannot fully function without help and reports from the public. If you see something, say something. An unaware employee population will fall for phishing attacks, and will never report it or know they are compromised. That's why we regularly perform penetration test exercises on our own employees – not just to catch anyone who is deficient in their security practices but to embed in every employee the need to be vigilant and exercise caution, even when an incoming email seems plausible. In sum, awareness training may not provide complete protection, but it is part of the equation that must be addressed by every organization.

Patch/vulnerability management is the third, and some say the most important, step that organizations must take. But like most security functions, patch management is only as good as the people behind it. Patches of critical vulnerabilities should be required within a short window.

The fourth step involves making sure an organization has a working enterprise-level **malware detection/prevention solution** that keeps machines and devices up to date with the most current definitions or software. According to Symantec, there are nearly one million new malware variants introduced every three days! That's why, like patch management, anti-malware updates

are critical. Similarly, IT departments need to review the security logs daily to check for anomalies and promptly report problems to top management.

Finally there have to be cyber security **policies and procedures** in place that are strongly supported, reviewed and enforced. Too often organizations view policies and procedures as a checkbox paper drill, which is a huge mistake. Good policies and procedures eliminate confusion in the aftermath or during an otherwise chaotic event.

As part of this, private and public sector organizations need strong, qualified individuals in the right positions. Unfortunately, many companies and organizations are settling for individuals who can talk their way into a Chief Information Security Officer (CISO) or Security Director role without having any real experience, or are asking others to look at the job as an "other duties as assigned" role. Having credentials, a strong background and practical experience is critical. Whether we are talking about a commercial company or a government agency, it is critical to have the right person in a position to inform executive leadership about real risks and the appropriate steps to mitigate them.

These five elements – strong passwords, security awareness training, patch and vulnerability management, malware prevention and detection solutions, and policies and procedures – serve as the foundation for a strong cyber security risk management program. We believe in them, and we follow them. This is not something extra we *ask* of our employees – it's something we absolutely require.

Looking past these five basic steps, one additional item that should not be overlooked is encryption. Without encryption, laptops, mobile devices and USB sticks that are lost can easily lead to a data breach. Encryption of sensitive information is equally important whether dealing with web applications, communications or a database. A note of caution with respect to encryption; it is not a silver bullet. If valid credentials are entered into the web application it must decrypt the data for the end user to be able to manipulate or consume the data. This is why it is critical that administrative access is limited and that web application vulnerabilities are continuously looked for, identified and remediated.

It's important to recognize that no one process or security software is fool-proof. That's why we also advocate a defense-in-depth approach, which means protecting a network with multiple security mechanisms. If one mechanism fails, another is in place to thwart the attack. It's similar to fortifying a government or even a sensitive private sector installation. You build a secure facility and have armed guards on the perimeter, but if a truck rams the gate you need to have additional protections on the inside of the complex as well. It's a layered security model. The more layers in place, the harder it is for an attacker to infiltrate. Having a web application firewall sitting behind a network-based firewall makes an attacker work twice as hard. Having the system hardened with anti-malware creates yet another opportunity for the security defenses to prevent an impending attack.

Once a strong risk management program is in place, there is an equally critical task facing organizations: *How and when to respond to and recover from an incident.* Our folks came up

with some common steps of **incident response** that serve as a helpful guide for us, and should be used by government agencies as well. These are:

1. **Preparation** – Prepare for an incident by opening lines of communication, having the proper documentation, and implementing an incident response team.
2. **Identification** – Next, answer the following question: Has something deviated from the norm causing an incident?
3. **Containment** – Prevent further damage and assess the scope of the incident.
4. **Eradication** – Remove and restore affected systems. Monitor fixes to assure malicious software and bad actors are removed.
5. **Recovery** – Bring systems safely back into production.
6. **Lessons Learned** – Identify who, what, where, why, and how the incident happened. What needs to be improved? What security policies and procedures need to be updated?

Underlying this strategy is continuous diagnostics and mitigation (CDM). We used to only talk about "continuous monitoring," which Telos has been involved with for many years and which, as the committee stated in its announcement for this hearing, was cited recently by OPM's Office of the Inspector General as being a basic security process where OPM's efforts have fallen short. But as noted above, the mitigation steps which an enterprise takes are also critical.

Continuous monitoring solved one problem (detection) but left out another (remediation). As organizations embraced the concept of continuous monitoring, continuous response remediation was the obvious next step. Extending the continuous monitoring framework to include automated methods for triggering remediation and response activity is essential. So now the more accurate and complete operative phrase is CDM. That is the current priority of Congress and of the Department of Homeland Security, which notes on its **website** that, "Congress established the CDM program to provide adequate, risk-based, and cost-effective cyber security and more efficiently allocate cyber security resources."

This hearing was also originally called to address **whether the voluntary cyber security standards (the "Framework") put forth by the National Institute of Standards and Technology (NIST) can truly be effective.** We continue to believe that the various critical infrastructure sectors are so important to our national defense, our national economy and our way of life that the government needs to do everything it can to promote best cyber security practices, such as those put forth by NIST. Most businesses would prefer that the government impose the fewest possible requirements on them. But how many breaches will it take before it is recognized that allowing the private sector – and especially critical infrastructure companies – to choose the path of least resistance creates an opportunity that might put our citizens' personal information at risk, put our critical infrastructures at risk and put our national economy at risk?

The hard reality is that the current NIST standards are purely voluntary, in part due to recognition by the Administration that there is insufficient support in Congress and the private sector to mandate stronger action. Various proposals to require stronger action were blocked in Congress a few years ago, and nothing seems to have changed. By comparison, the German Parliament last year passed legislation requiring critical infrastructure institutions to implement minimum information security practices or face fines. Once additional implementing legislation

is passed, more than 2,000 essential service providers will have two years to comply with the new requirements. The German agency charged with enforcing these requirements will also be given the resources to expand to cover these new obligations, which will include evaluating reports of possible cyber-attacks on critical infrastructure.

Since Congress and the Administration have not taken the same strong steps that Germany is now taking, everything possible must be done to incentivize companies to *voluntarily* take the strongest possible actions to protect themselves, which includes following the NIST standards. Make no mistake, the NIST standards are very good…but companies must follow them even though they are voluntary.

One promising area of incentivizing companies to take strong steps on their own is the growth of the cyber insurance market. One of our experts noted several years ago that, as we see more frequent cyber security breaches, the cyber insurance industry will mature with each new data point it collects, and thus be able to more easily determine appropriate coverage, premiums, etc. Moreover, as insurance companies get their arms around this cyber security actuarial data, they will also want to have insight to what their clients are doing to protect themselves from cyber attacks. That is, are their clients employing adequate controls and security practices? Are these organizations applying sufficient ongoing care in the protection of their systems and data? Are their clients utilizing the NIST cyber security framework standards which, while voluntary, are nonetheless standards insurance companies can encourage, incentivize or even require their customers to follow? If that happens, and if it happens more frequently, then we could see greater market pressure brought to bear to effectively "require" other companies to do the same.

That is certainly better than allowing companies to do the bare minimum to protect themselves and those who do business with them. We need them to do the most they possibly can, not the least. In this way, market forces and the fear of legal liability will make these voluntary standards the de facto standards for companies to demonstrate to insurers or in court that they have exercised all due care to protect their assets and customers.

This rescheduled hearing also now seeks **feedback on the recently enacted Cybersecurity Act of 2015**, which was included in the Consolidated Appropriations Act to fund federal departments and agencies for the remainder of Fiscal Year 2016. As the committee members know, this law provides certain incentives to encourage private sector companies to voluntarily share cyber threat information with the federal government and/or with other private sector companies. We believe this new law overall is a net positive – threat information sharing is a good goal…but in practice it is much more complicated and it is difficult to achieve effective results.

Our first concern about the new law is, like the NIST Framework discussed earlier, it doesn't go far enough because of its purely voluntary nature. As has been shown in the experiences of those who participate in Information Sharing and Analysis Centers (ISACs), some companies just don't want to participate and disclose information about any weaknesses or vulnerabilities they might have. It's human nature not to want to disclose bad news to stockholders, investors, customers, and others if they don't have to – some companies will want to privately address any problems, without the inherent "bad publicity" of disclosure. The same holds true with respect to limited disclosure of confidential threat information. The Securities and Exchange

Commission has been making an effort to require greater disclosure of breaches, but timely disclosure to the government or other companies of confidential vulnerability or threat information is another matter. If a company chooses not to participate, it may be withholding vital threat information and thus putting other companies and individual citizens at risk.

Ironically, the law actually may create a "Catch 22" – some organizations may share *too much* information in an attempt to maximize liability protections, potentially resulting in too much data being shared and potentially putting personally identifiable information (PII) at risk.

Only time will tell if this latter concern is borne out, but we continue to believe the former concern about the law's purely voluntary nature is a very real one – it only takes one company's failure to act voluntarily to put many others at risk. We believe that, as with the NIST Framework, stronger market force incentives will be needed to encourage greater participation.

While it is not within the scope of this hearing, one final area I would like to address in this written statement is the need for the United States government to adequately fund cyber and information security. Making cyber security a priority to make our nation secure means making sure the government buys the best cyber security solutions it can get, not the cheapest. The **Lowest Priced Technically Acceptable** (LPTA) contracting environment we find ourselves in today often leads to awarding critical contracts to lowest cost bidders. The government should be looking for the best *value*, especially when it comes to cyber security. Congress needs to ask each agency what they need to properly protect their systems and then fund it.

Neglecting to properly fund our nation's cyber defense is severely shortsighted. Several years ago, our Government leaders argued correctly that cyber was the fifth warfighting domain along with land, sea, air, and space. Arguably, cyber is the most difficult domain to defend, and yet, we continue to undercut it, undermining our national security.

As an example, the President's proposed Fiscal Year 2016 Budget allocated $560 billion for the Department of Defense. Of that $560 billion, the Army was to be given $146 billion, the Navy $152 billion, and Air Force about the same. By comparison, the U.S. Cyber Command, with its incredibly challenging responsibilities to protect the fifth warfighting domain, was allotted about $462 million – less than 1/1000 of the total DoD budget. This funding disparity did not significantly change in the final FY 2016 appropriations legislation enacted in December. This failure to provide the funding needed to meet the cyber challenge applies to both military and civilian departments and agencies. As a result, we are vulnerable throughout the government.

Many private companies understand the challenges of protecting themselves from cyber threats, and are taking action. Financial services firms in general are especially battening down their hatches; they see the cyber risk and are being responsive to their customers and stakeholders. ***Forbes* recently summarized various media accounts of such actions,** noting that J.P. Morgan Chase & Co. expects its cyber security spending to be around $500 million in 2016, more than double the $250 million it spent in 2014. *Forbes* also reported that Bank of America Corp. CEO Brian Moynihan said previously his company would spend $400 million on cyber security in 2015, that Citibank's IT security budget reportedly tops $300 million, and that Wells Fargo is

reported to spend roughly $250 million a year on cyber security. These institutions understand that devoting the resources necessary to protect their systems is absolutely critical.

Such expenditures produce results. According to a **recent Veracode report** comparing the state of software security by industry vertical, **government agencies fix fewer than one-third of all detected [software security] problems … by comparison, financial services fixed 81% of detected problems, while manufacturing fixed 65%**. In light of the variance in funding levels between the government and private industry, it is no surprise that once detected, two-thirds of the software security problems in government systems are left unresolved. Private industry is funding cyber security like they're taking the issue seriously. The federal government is not.

Defending our nation in cyberspace requires a long-term national effort and commitment, much like the Space Race -- we have the equivalent of a cyber-race to the moon on our hands, and we are falling behind. This is the reality, and our Government leaders and Congress need to stop just talking cyber, and to start appropriately funding it.

In closing, on behalf of Telos, I appreciate this opportunity to share with you our perspective on these important issues, and I'd be glad to answer any questions you might have.

# # #