Cybersecurity Thought Leader Interview Series:
Q&A with Glenn S. Gerstell, National Security Agency

Glenn S. Gerstell *is General Counsel of the National Security Agency. Mr. Gerstell has four decades of private practice experience. He has also served as a member of the National Infrastructure Advisory Council, a member of the Council on Foreign Relations and the American Academy of Diplomacy. This interview with Mr. Gerstell was conducted and condensed by Craig A. Newman, the chair of Patterson Belknap's data security practice.*

Q. Last year, you noted that cyber vulnerability is one of the biggest strategic threats to the U.S., and in fact, some government officials place cyber threats ahead of terrorism. Do you think the true nature of this threat – in business and economic terms – is fully realized by the private sector?

A. In February, the Director of National Intelligence once again listed cyber threats first among global threats in his annual Worldwide Threat Assessment, thus underscoring the importance of cybersecurity to our nation's wellbeing. I think that the private sector is broadly aware of the nature of the threat posed by malicious cyber actors. This is an issue that has been well studied; it's in the news every day, and (partly because of its ubiquity) the cyber threat is probably more thoroughly recognized than are many other potential dangers.

With that said, outside of certain industries - such as the financial and energy sectors, for example – I don't think that many businesses fully appreciate their own vulnerability to cyber threats. Unlike many other dangers, cyber is a threat that doesn't always manifest itself immediately, or perhaps at all. Most individuals and many businesses lacking sophisticated intrusion detection are unlikely to have any idea that their device or network has been compromised. Moreover, many individuals and small businesses, perhaps understandably, assume that they're just small fish - too unimportant or uninteresting to be a target of malicious cyber actors - but we've seen that in some cases their very vulnerability makes them an

easy target. Finally, some businesses are well aware of their own cyber vulnerability, but are simply too under resourced to address the problem.

Q. What are the top cyber initiatives on the NSA's agenda, at least those you can speak about publicly?

A. Although not subject to the same level of public attention as its foreign intelligence operations, cybersecurity has long been one of NSA's two primary missions. We are charged with a variety of functions related to the security of national security systems and the information stored and carried on those networks. NSA is responsible for assisting in the security of all classified government networks along with those unclassified networks that involve intelligence activities, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or equipment that is critical to military or intelligence missions. This could include, for example, the network of a company with a Department of Defense contract. Among other things, NSA sets security standards and conducts vulnerability assessments for these systems. In undertaking this work, we need to stay a step ahead of sophisticated adversary nations and other malicious cyber actors, who make our networks their daily targets.

As most are aware, the pace of change in cyberspace is incredibly rapid. We therefore have to work hard to stay on top of new developments and technologies. In order to remain at the forefront of the cybersecurity field, NSA must recruit and develop world class cyber talent. As you can imagine, our employees' skillsets are highly sought after in the private sector, and so one of our key initiatives has been to take steps to encourage STEM employees [those employees with disciplines in science, technology, engineering and mathematics] to remain with the Agency.

We've introduced financial incentives for certain skill fields to enhance our ability to compete relative to the private sector, but we continue to look for ways to build and retain a talented cybersecurity workforce.

NSA has also been examining ways to share our cybersecurity insights with the private sector and other government agencies in a real, usable way. We've recognized the need to shift the focus from response, mitigation, and recovery efforts after a cyber event has occurred to a more proactive posture. To accomplish that, it is essential that cyber threat information is shared as quickly and broadly as possible.

Unfortunately, this objective is not as easy as it sounds. What many might not realize is that some of NSA's deepest and most consequential cybersecurity insights are developed as a result of information collected pursuant to our foreign intelligence mission. As a result, sensitive sources and methods are often implicated when we share cyber threat information. Alerting victims of cyberattacks and providing proactive warnings about vulnerabilities may seem

straightforward, and we certainly endeavor to do so working with our federal partners at the Federal Bureau of Investigation and the Department of Homeland Security. We do, however, have to consider whether disclosure could cost us access to information about adversaries who might be involved in malicious cyber activities today, but who could be engaged in terrorism or weapons proliferation tomorrow.

In addition to these classification challenges, there are institutional hurdles to rapid information sharing. Our systems simply were not designed for instantaneous information sharing with the private sector, nor are private sector systems configured to interface appropriately with government ones. Before we can disseminate cyber threat information, we have to determine whether sensitive sources and methods may be implicated; examine legal and policy restrictions to ensure sharing is lawful and appropriate; address classification concerns; and format and present the information in a manner useful to those receiving it. This process also highlights another challenge we face: given the dispersal of responsibilities for cyber throughout the federal government, NSA is not in privity with the individual network owners who need to act upon our cyber threat information.

The good news is that we're working hard to confront these challenges and we're making progress. Historically, much of the process for sharing cybersecurity information with the private sector was performed manually. We've now begun to put in place automated processes to produce cyber threat indicators, format them for sharing, and send them to the DHS for dissemination to the rest of the government and the private sector via their Automated Indicator Sharing initiative. We also recently combined our foreign intelligence and information assurance operations into one directorate so that we can share insights more quickly across our mission spaces and address cybersecurity in an integrated way. Additional work is needed, but I'm encouraged by the amount of effort being devoted to this initiative.

Q. The Cybersecurity Information Sharing Act – passed by Congress in 2015 – is aimed at fostering sharing of threat intelligence between the public and private sectors. In what ways do you think information sharing can be enhanced to create a more coordinated public-private sector approach to cybersecurity readiness? Is the UK's National Cybersecurity Centre a model we should be thinking about more seriously in the U.S.?

A. CISA was certainly a positive step toward increased cybersecurity information sharing between the public and private sectors, but I believe even its advocates recognize that it does not represent a complete solution. Cybersecurity in today's environment is a difficult problem, and we need to continue to look for ways to improve. That includes scrutinizing how cybersecurity responsibilities are assigned across the government and how those assignments impact information sharing.

Many different advocacy groups, panels of experts, and members of Congress have studied how best to organize the government to address the cyber threat. There are varied opinions on the best approach, but the UK's NCSC model is at least worthy of examination. I'm not suggesting we adopt that model, but I do think our public discussion over the right approach can be informed by looking at what other countries have done. Like the U.S., the UK used to have various entities, all with disparate responsibilities for cybersecurity. The UK brought these responsibilities together under one roof and housed that agency within the Government Communications Headquarters, which is the UK's version of NSA. The NCSC is intended to act as a bridge between industry and government, providing a unified source of advice, guidance, and support on cybersecurity and management of cyber incidents. Many countries are taking a similar approach to that of the UK, including centralizing cybersecurity authorities in one organization. There are obvious benefits and drawbacks to adopting such an approach. For example, pulling cyber expertise together in one organization might enable the government to generate cybersecurity insights more quickly, but there are cultural, political, legal, and structural challenges that such a model would face in the U.S. Nevertheless, despite many conflicting opinions on the subject, I think everyone has agreed that we need a more integrated approach to the cyber threat.

Q. What is the most daunting cyber threat you see over the next year?

A. Let me pick up on my prior response to make the obvious point that if an integrated and effective approach to the cyber threat were easy to implement, we'd have a solution already. Continued dialogue among Congress, the private sector and the executive branch is needed before a clear consensus emerges. Every report issued on cyber threats reflects an exponential increase in malicious cyber activity year after year. We are seeing more determined nation states adding additional cyber resources to what they view as a strategic way to advance their goals, and cyber criminals continue their nefarious acts, in part because of low costs of entry and reduced chances of getting caught. Unfortunately, I think this all means that as a country we are going to have to live with a rising cyber threat for a while before we collectively surmount it.

With that as a backdrop, I'd like to highlight two cyber threats that I see as presenting significant challenges in the near term. These two threats, in particular, underscore the importance of positioning the federal government to prevent and, if needed, respond to a major cyber event.

The first threat is the exponential increase in the complexity of cybersecurity created by the Internet of Things. I don't think that we, as a society, have kept up in terms of standards, regulations, or laws governing IoT products. Therefore, many of these IoT products are developed in a way that doesn't prioritize cybersecurity, making them vulnerable to exploitation. Those flaws, combined with the sheer volume of connected devices and networks, has led to a proliferation of

cyber vulnerabilities and an expansion of the consequences flowing from that vulnerability.

Second, I fear it is only a matter of time before we see malicious cyber activity that involves the wholesale destruction or manipulation of data. Many of our critical institutions here in the U.S. rely heavily, if not entirely, upon electronic information. If their electronic data becomes unavailable or unreliable, such an attack could undermine public confidence in key institutions. Should this occur, the consequences could be disastrous.

Q. In your role, you are responsible for legal oversight of all NSA activities. What makes you lose sleep?

A. With respect to NSA's execution of its mission, I can honestly say that I sleep soundly. That response is not an attempt to avoid the question; rather, in my experience, NSA has been able - due to the recognized importance of its mission to the nation - to recruit and retain high- caliber employees who demonstrate not only superb technical excellence, but also and equally importantly, a commitment to compliance and to the rule of law. If I'm awake at night, it's a result of external threats facing our country today. As part of the national security community, our mission is to produce intelligence that will help protect the homeland. In this role, however, that means I often have a detailed view into the plans and intentions of our adversaries. As you can imagine, this can be a troubling perspective to have. But ultimately I do get a good night's sleep since I have confidence in NSA and our partners across the federal government.