QUESTION FOR THE RECORD

TO

PAUL ROSENZWEIG

FOLLOWING THE SENATE JUDICIARY COMMITTEE HEARING:

"THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION AND THE PUBLIC'S RIGHT TO KNOW."

HELD ON MARCH 13, 2012

FROM SENATOR CHARLES GRASSLEY AND SENATOR SHELDON WHITEHOUSE:

Question: During the hearing, you were asked a two-part question by Senator Grassley. However, because of time constraints, you were only able to give abbreviated answers. Please provide complete answers to the following:

> First, describe the type of information involved when a business shares cyber threat information with the government.
>
> Second, describe the type of damage that you believe would be done to the business sharing the information and to our Country, if that cyber threat information was made public.

Answer: Information shared to reflect a cyber threat: As I said at the hearing cyber threat and vulnerability information generally falls into two bundles – the malicious code/threat itself and the data substrate in which the code arrived. A more formal analysis would expand on that shorthand summary in the following way:

The fundamental architecture of the Internet gives rise to the difficulty of distinction – it is a problem that is, in effect, built into the system. In a short hand way, all the 1s and 0s look the same.

Any successful cyber attack or intrusion requires "a vulnerability, access to that vulnerability, and a payload to be executed."[1] But in practice the first two parts of that equation (identifying a vulnerability and gaining access to it) are the same no matter what the payload that is to be delivered. Thus, for those attempting a defense, it is virtually impossible to distinguish *ex ante* between different types of intrusions because they all look the same on the front end: cyber espionage, where the intrusion is a payload that seeks to hide itself and exfiltrate classified data; cyber theft, where the object is stealing unclassified financial data; and a full-scale cyber attack, where the payload left behind may lie dormant for years before it is activated and causes grave cyber damage, cannot be readily distinguished as the software traffic is entering a system. The

[1] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 4 *Journal of National Security Law & Policy*, 63 (2010).

difference arises only when the effects are felt. The closest kinetic world analogy would be something like never being able to tell whether the plane flying across your border was a friendly commercial aircraft, a spy plane, or a bomber.

This is not a readily soluble problem. All computer programs, including those used in cyber intrusions, are written in a programming language, often known as a source code. That source code is then compiled into the binary language understood by computers. To execute the program, or code, the computer reads the directions of the compiled binary language. This complex rendering from source code to executable instructions makes reading lines of computer code to discern their effect, in practice impossible. While different types of airplanes look functionally distinct from each other, computer code does not.

This circumstance changes only down the road, when an intrusion has been activated in one instance and the implementing code analyzed to reverse engineer the programming. Once that happens, a threat signature can be developed – and it is that threat signature that lies at the core of the pending information sharing proposals. Likewise, the analysis will often identify the particular gap, or vulnerability that is exploitable – a vulnerability that ought to be plugged once identified.

The information in question will relate, broadly speaking, either to specific threats from external actors (for example, knowledge from an insider that an intrusion is planned) or to specific vulnerabilities (for example, the identification of a security gap in a particular piece of software). In both situations, the evidence of the threat or vulnerability can come in one of two forms: either non-personalized information related to changes in types of activity on the network, or personalized information about the actions of a specific individual or group of individuals.

Network traffic information can relate to suspicious packets, including ports, protocols, and routing information; specific virus/other malware signatures; IP addresses; and the identification of particularly suspect domains or servers. Personally Identifiable Information (PII) includes more person-specific types of information such as identifying web sites accessed; times and locations of logins/account access; discrepancies in user names; or content of communications. It is typically related to a specific malfeasant activity (such as an attempted fraud, identify theft or the transfer of terrorist finances).

Once threats and vulnerabilities are known, we want them widely distributed. Thus, the first "bundle" of information constituting cyber threat and vulnerability information will be identified malicious source code and/or specific vulnerabilities within system that are capable of being exploited.

The other "bundle" of information will be the surrounding data within which the malicious code is secreted – in other words, the non-malicious code that represents the legitimate data stream being screened. Building on the description above, it is the non-malicious web sites accessed; the correct user names; or the legitimate IP addresses. It can also be the content within which the code arrives – an Excel spreadsheet for example, or perhaps a Word document (both have been used in recent years for the intrusion of a malicious Trojan horse program). It might be the email text with legitimate information that prefaces a malicious phising hot link.

This second bundle of information can be equally critical in identifying a vulnerability or threat methodology. Knowing the particular nature of an attack allows us to educate recipients on potential vectors of attack. But, critically, describing those vectors may not (indeed typically will not) require knowledge of the actual content – the nature of the attack is independent of the content data within which the attack resides.

Damage from publicizing threat and vulnerability information: Just as there is a market in producing cybersecurity there is also a market in producing cyber vulnerabilities. Knowledge of those vulnerabilities is a valuable commodity with commercial value. Should anyone doubt that there is such a private market consider the sale of zero-day exploits (that is, previously unknown vulnerabilities). Cyber hacker entrepreneurs expend great intellectual capital in discovering these exploits and marketing them on the black market. Truly unique and unusual zero-day exploits can sell for as much as $50,000. There is even a royalty provision in some sales where the discoverer gets a continuing payment for as long as the vulnerability remains unpatched.[2]

Given how difficult it is to discover vulnerabilities of this sort, it follows that the premature or unnecessary public disclosure of those vulnerabilities has the potential for doing grave damage to security interests. This is so because, in a resource-constrained world, even after a vulnerability is discovered it may take a period of time (sometimes quite substantial) before that vulnerability can be patched.

To cite a notable recent example, many of our legacy manufacturing control systems (known as SCADA systems) are vulnerable. The recent Stuxnet attack on Iran demonstrated that. But these SCADA systems are also quite old, deeply integrated into production processes and, unfortunately, difficult to patch. Yet replacing them is exceedingly expensive. The realistic prospect is that many of their vulnerabilities will remain in existence for a substantial period of time.

Fortunately, given the complexity of most SCADA systems it is highly unlikely that particular vulnerabilities will be readily discovered or widely known. Public disclosure of those vulnerabilities would have the perverse effect of disseminating information that, in any rational world, the system operator (and all of its customers) desperately hope to have remain confidential.

FROM SENATOR CHARLES GRASSLEY:

Question: Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony and/or responding to the testimony of the other witnesses.

Answer: Thank you very much for the opportunity to amplify on my answers. However, after reviewing the hearing transcript and the written testimony of the other witnesses I do not have any additional thoughts to add to the Committee's record.

[2] Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*, (Independent Security Evaluators 2007), http://weis2007.econinfosec.org/papers/29.pdf.

FROM SENATOR AMY KLOBUCHAR

Question: The Supreme Court decision in *Milner* limited the extent to which critical infrastructure information can be shielded by FOIA Exemption 2. Given that ruling, how can the current FOIA statutory scheme best be modified in order to protect critical government security information?

Answer: Since *Milner* there has been significant confusion within the Federal government. Despite the suggestion of the Supreme Court that other exemptions might be applicable, it has become clear that a great deal of critical security information that it is reasonable to withhold has become subject to disclosure. In practice this has led separate programs to seek so-called (b)(3) exemptions for specific types of information. In general, that sort of piece-meal approach ought to be disfavored and Congress should prefer a more uniform response. The most reasonable solution, in my judgment, would be for Congress to restore the *status quo ante* by legislatively enacting the old "high 2" exemption into law – perhaps limited by adopting a definition of critical infrastructure to which the exemption might apply. One model for an appropriate definition would be that used in the Homeland Security Act to define protected critical infrastructure information.