Response to the Request for Information dated 2/26/2013
"Developing a Framework to Improve Critical Infrastructure Cybersecurity"
Issued by the National Institute for Standards and Technology

April 8, 2013

Mandiant protects the assets of the world's most respected brands and government agencies from advanced cyber attackers. In addition to responding to high-profile computer security incidents, such as the New York Times, we equip security organizations with the tools, intelligence and expertise required to find and stop attackers who would otherwise roam freely on their networks. We serve more than 30% of the Fortune 100.

During the course of our work with our many clients Mandiant has gathered evidence of fraud, theft, child pornography, insider sabotage, financial misappropriations and economic espionage appearing to originate both domestically as well as several different foreign nations. We have managed incidents caused by motivated individuals as well as well-organized, generously funded and sometimes state-sponsored groups. These groups are differentiated from "consumer-grade" or commodity threats by their targeted nature. They target a particular organization for a particular reason, not just harvesting personally identifiable information or credit card information.

It is reasonable to assume that, if an advanced attacker targets a company, a breach is inevitable. No amount of perimeter, network or application security will stop an advanced, determined threat actor. That surprises many people, but it is the undeniable truth, and a direct result of the gap between our ability to defend ourselves and our adversaries' ability to circumvent those defenses.

Any successful cybersecurity framework needs to promote a system that helps companies defend against emerging threats. This requires updating the view of incident response to be an ongoing process rather than an occasional one, where organizations build CIRT (Computer Incident Response Team) capabilities and interact with other organizations for improved mutual defensive postures. In Mandiant's view, a successful cybersecurity framework also requires a strong national policy that promotes the sharing of actionable threat intelligence and protects companies that share this valuable information.

Threat Intelligence Sharing

The Framework that NIST is tasked with drafting and the related programs DHS is developing should establish a system that tracks the most recent advanced threats and distributes information about those threats to the people in a position to do something about them. Both the government and some private sector companies have much of this information, and we need to create a way in which they can share actionable intelligence in a standard, machine-readable way that does not diminish the effectiveness of or betray our intelligence mission. Sharing threat intelligence will promote an aggressive, dynamic "learning system" of cybersecurity for the nation. Effective intelligence sharing:

1 – Acts as an early warning system giving potential victims advance notice of threats;
2 – Empowers the private sector to defend itself more effectively; and
3 – Significantly reduces the duration and impact of breaches, should they occur.

About two-thirds of the breaches Mandiant responds to are first detected by a third party – usually the government – not the victim companies. That means that a majority of the companies we assist had no idea they had been compromised until law enforcement or a business partner notified them. While informing the victim is critical, taking advantage of the knowledge of the threat as an opportunity to strengthen the defenses of other potential victims is what is currently needed. Threat information, if shared consistently with the right people, could be used to prevent or mitigate the impact of these breaches instead of merely notifying victims long after their intellectual property has been stolen.

Information sharing also needs to occur within and among private sector participants. While we have witnessed some advancement in coordination within the private sector, especially in the defense industrial base and the financial services sectors, U.S. companies remain at a severe disadvantage until they can access and utilize all of the information available.

In promoting the sharing of threat intelligence, it is equally critical that we devise a means to standardize the information shared so it can be provided "at network speed" to make timely use of the intelligence. We need these threats to be reduced to computer code to effectively safeguard the identities of victims and share freely threat intelligence from anonymous sources. If we standardize how we communicate threat intelligence, we will expedite the implementation of our defenses, create more reliable and effective intelligence, and empower the private sector to share amongst themselves in a more productive manner. The Framework would benefit from the implementation of a data sharing standard such as Mandiant's OpenIOC format and compatible standards like the STIX schema from MITRE, accelerating the intelligence sharing process.

Continuous Incident Response Process

Most existing incident response guidelines do not effectively address persistent adversaries. Existing guidelines outline incident response as an occasional workflow that teams enter into and

complete, finding a compromised system remediating it and returning to status quo. Mandiant has found that successful organizations treat incident detection, response and containment of adversaries as an ongoing process. Constant vigilance and rapid response is necessary to keep an organization secure, because persistent adversaries with specific goals will continue to return until their goal is complete, regardless of the actions of defenders.

At Mandiant we have found that focusing on detection has been a successful strategy. By combining host and network-based visibility with enhanced and centrally aggregated logging we have seen how the application of actionable intelligence and indicators of compromise can support a coordinated response across the enterprise. Containment should occur in a structured, targeted, threat remediation event, rather than piecemeal; pulling the adversary out by the roots in one fell swoop rather than leaving incidents of infection to provide footholds for future access.

In most existing incident response workflows, the incident is deemed "complete" and most workflows go into a "lessons learned" phase after remediation or containment. We instead feel that the Framework should support organizations cycling back into detection without any lapse in time, as most persistent adversaries will attempt to regain access in short order. Any framework that is going to be useful against persistent adversaries needs to reflect the idea of incident response as a consistent process rather than an isolated one, and any new frameworks developed should reflect this characteristic of successful organizations.

In conclusion, while private industry will not always win the battles being fought in cyberspace, we can drastically narrow the security gap by sharing threat intelligence in a uniform and productive way and maturing incident response into a recurring component of any risk mitigation plan. To gain ground against the increasingly numerous and sophisticated attacks draining this nation of its most valuable assets, this Framework must encourage and facilitate the public/private exchange of threat intelligence and encourage evolved thinking in incident response team workflows. By establishing a system where the private and public sectors share and proactively use accurate and timely threat intelligence, the U.S. will build a dynamic cyber-defense system that grows smarter and more capable by the day.