The Department of Commerce and the Department of Homeland Security (DHS) issued a Request for Comment on September 21 seeking industry responses to a range of queries involving possible standards for addressing botnet infections. The federal government issued the request in response to its concerns over the potential economic impact of botnets and the harm they can cause to computer systems, consumers, businesses, and government systems. The request is focused on developing a “voluntary industry code of conduct” to “address the detection, notification and mitigation of botnets.” The request has received media and industry attention in recent weeks, and responses may help establish industry best practices that will impact public debate as well as liability and insurance industry expectations.

What Are Botnets?

Botnets are a form of malicious programming that can be used to remotely control computers, assembling infected computers into a network that executes the commands of the botnet program’s controllers. Botnets can be used to attack other networks or computers, or simply to offer a window into the infected systems and the private information of their users. Botnets pose significant threats to consumers, industry, and government interests, as they enable malicious actors to utilize the information obtained for nefarious and often criminal purposes, including identity theft, in a manner that can be difficult to detect. Networks made of compromised computers also can be used to send spam and illegal content, and even to engage in denial of service attacks against governments or private enterprise.

What Information Is the Federal Government Requesting?

DHS and the Department of Commerce are seeking comments about the most effective ways of dealing with botnets. Although the request is made in the context of botnets, it includes other malware (malicious software consisting of programming designed to disrupt operation, gather information, or gain unauthorized access to system resources) within its scope as well. The request suggests several options for addressing the threat, including a proposal for liability protection for compliant companies and the creation of a resource center to assist infected consumers, but concentrates primarily on the value of voluntary compliance standards. The request poses a range of detailed questions, which focus on:

1. The utility of a voluntary code of conduct to address the botnet threat
2. The potential means for private entities to assist in the detection and prevention of botnets and other malware
3. The options for notifying consumers of infection
4. The types of incentives that might encourage private participation in a code of compliance
5. The types of resources that should be established in the United States to assist with notifications and the most effective location (whether government or private) for housing such resources

Under all of these sections, the agencies seek to learn more about current industry practices and options for improving and universalizing approaches to protecting and assisting consumers.

What Impact Will This Request Have on Industry and Consumers?

The request is a solicitation of information from all stakeholders. It has the potential to guide government regulatory action in the area of consumer protection and industry cooperation when dealing with botnets specifically and malware more generally.

The bulk of official government cybersecurity resources are focused on protecting critical infrastructure, such as the power grid and nuclear facilities, and the Department of Commerce recently has articulated a need to cooperate with the “Internet and Information

---

1 “Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware,” Federal Register 76 (21 September 2011): 58466-58469. Comments are due by November 4, 2011, to Consumer_Notice_RFI@nist.gov.

Continued on page 2...
Federal Government Issues Request for Comment...

Continued from page 1...

Innovation Sector”—what it calls I3S—to improve security more broadly.\(^2\) The Department of Commerce describes I3S generally as including any “functions and services that create or utilize the Internet or networking services.”\(^3\) The request reflects the Administration’s apparent policy to seek voluntary industry cooperation whenever possible in confronting cyber threats to I3S. According to the report, the Department of Commerce sees itself (and the government more broadly) as playing a key role in encouraging voluntary compliance standards.

The request provides industry with the opportunity to engage policymakers in the early stages of regulation in this area. It is possible that, as cyber threats become more serious and costly to public and private interests, Congress may impose strict statutory requirements calling for significant government regulation in this area. More than a mundane regulatory request, therefore, the current solicitation has the potential to establish a baseline for future debate about best practices for countering cyber threats from botnets and other sources. It may prove influential in establishing norms when the government seeks to regulate and legislate in this area.

In addition to framing future debates, the ideas and concepts that emerge in the coming months also may have legal and insurance ramifications. Where other standards are lacking, as is the case with many facets of cyber security, industry best practices can become the default standard used in the courts to determine whether a party is liable for failing to meet its duties to consumers or other counterparties. As new cyber security standards emerge, they are likely to set the judicial framework for determining whether a party has acted sufficiently to protect the systems and information of those with whom it interacts. The judicial framework could have considerable implications for companies in the context of fiduciary duties and civil liability.

Moreover, the emerging cyber insurance market might take its cues from both the standards that may surface from the request and the broader discussion concerning consumer protections that is occurring at this time. As industry insures itself against suits for privacy disclosure and other cyber-related events, insurance companies will look to legal standards and industry practice to determine policy qualification requirements. In short, the standards established now will drive investment requirements for industry with respect to cyber and data security and also will establish new regulatory regimes charged with ensuring compliance with those standards.

**Conclusion**

The Request for Comment offers an opportunity for the private sector to inform government thinking on a range of issues related to botnets and malware. Stakeholders who engage early in this discussion by playing an active role in shaping the government’s policy may have the ability to impact commercial practice and legal standards that develop as a result of government action in this area.

For further questions about the Request for Comment or other related matters, please contact Don Vieira at dvieira@wsgr.com or 202-973-8800, Lydia Parnes at lparnes@wsgr.com or 202-973-8800, or Brock Dahl at bdahl@wsgr.com or 650-493-9300.

---


\(^3\) IPTF, vi.