FISH.
FISH & RICHARDSON

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005
202 783 5070 main
202 783 2331 fax

Steven A. Bowers
Principal
Bowers@fr.com
202 626 6386 direct

VIA FEDEX

The Honorable William J. Baer, Esq.
Office of the Assistant Attorney General
Antitrust Division
Department of Justice
Main Justice Building
Room 3109
950 Pennsylvania Ave., N.W.
Washington, DC 20530

July 1, 2014

Dear Mr. Baer,

I am writing to you on behalf of our client, CyberPoint International LLC ("CyberPoint"), to request a business review letter from the Antitrust Division of the Department of Justice, pursuant to 28 C.F.R. § 50.6 and the Department of Justice and Federal Trade Commission Antitrust Policy Statement on Sharing of Cybersecurity Information (April 10, 2014) (hereinafter, "DoJ and FTC Antitrust Policy Statement"). This request for a business review letter is for a proposed cyber threat information sharing system developed for SecurityStarfish, LLC, an affiliated company of CyberPoint, called "SecurityStarfish."

I. Background

A. CyberPoint International LLC

Founded in 2009, CyberPoint supports a broad array of commercial, U.S. Federal Government, and international customers. Across these customer domains and around the globe, CyberPoint has been helping organizations defend their critical systems and infrastructure from advanced exploitation techniques and the kinds of sophisticated threats where commodity solutions are inadequate. It offers an array of cyber security services and solutions, including malware analysis and reverse engineering; digital forensics and incident response; and risk analysis and vulnerability assessments. CyberPoint's U.S. headquarters is located in Baltimore, Maryland, and CyberPoint also has permanent offices in Abu Dhabi. *See* http://cyberpointllc.com/. CyberPoint owns the pending patent application for the system's anonymization technology and is the majority shareholder of SecurityStarfish, LLC.

B. The Importance of Information Sharing to Cybersecurity

CyberPoint understands that disruption or manipulation of information systems could have dramatic economic and security consequences for both U.S. and global security. The threat

in cyberspace is evolving in sophistication and severity. Adversaries regularly collaborate in an efficient black market, sharing vulnerabilities, exploits, and target profiles. Attacks used against one company are routinely used with little or no modification against sector peers and firms in other sectors. Adversaries also exploit the supply chain to reach larger players whose compromise offers more substantial rewards.

Adversaries have become adept at identifying vulnerable targets and launching effective attacks. They are agile in adapting their attacks to avoid defenses, thereby forcing their victims into a reactive posture that fails to defeat attacks. Without accurate and timely intelligence on cyber threats, and on attacks focused on a particular industry or region, no amount of reactive cyber defense can prevent adversaries from achieving an unacceptable level of success.

Recognizing the importance of information sharing in combating cyber threats, the Department of Justice and Federal Trade Commission stated in its Antitrust Policy Statement on Sharing of Cybersecurity Information:

> Cyber threats are becoming increasingly more common, more sophisticated, and more dangerous. ***One way that private entities may defend against cyber attacks is by sharing technical cyber threat information – such as threat signatures, indicators, and alerts – with each other.***
>
> ...
>
> Core features of our nation's cyber security strategy are to improve our resilience to cyber incidents and to reduce and defend against cyber threats. ***One way to make progress on these fronts is by increasing cyber threat information sharing between the government and industry, and among industry participants.***

DoJ and FTC Antitrust Policy Statement at 1, 2 (emphasis added).

CyberPoint's proposed SecurityStarfish information sharing system, to be deployed by SecurityStarfish, LLC, is designed to address shortfalls in conventional, legacy information-sharing services, while operating within the framework set forth in the DoJ and FTC Antitrust Policy Statement.

II. Overview of the Proposed SecurityStarfish Information Sharing System

The DoJ and FTC Antitrust Policy Statement states that, "[i]n particular, the sharing of information about cyber security threats, such as incident or threat reports, indicators, threat signatures, and alerts (collectively, 'cyber threat information') among these [private] entities has the potential to greatly improve the safety of our systems." DoJ and FTC Antitrust Policy Statement at 3. Consistent with the DoJ and FTC Antitrust Policy Statement, SecurityStarfish, LLC has made information-sharing, via incident reports shared among members, a centerpiece of the proposed system.

The SecurityStarfish system is designed to allow members to share threat and incident data, attack information and remediation solutions to help define more-effective strategies across industries to prevent successful attacks. Anonymously-sourced incident reports focus on cyber activity within users' business sectors, regions, and technologies to provide data on current attack actors, trends, and attack vectors, producing a predictive view of likely threats before users are attacked. Intelligence on current attack actors, targets and trends within an industry sector helps corporate-level staff assess their organization's security posture, evaluate the effectiveness of their defenses, and direct budgets in an efficient, targeted manner. Knowledge of what is happening within a sector and across other sectors (including developments in the increasingly important cloud and mobile sectors) enables users to allocate limited resources with maximum effectiveness.

III. The Proposed SecurityStarfish Information Sharing Mechanism (Incident Reports)

A critical component of SecurityStarfish's information sharing is that members can share incident reports with complete anonymity. No attributable data are ever sent to the service during an incident-report submission transaction. All such data stay on the client's side. Human review prior to submission ensures that the data are completely anonymized. Thus, the user has final control over all content before it is sent. Private encryption keys are generated and maintained by the client-side application so that only the client can decrypt attributable data fields. SecurityStarfish also makes submission as easy as possible by automating attributable-data term removal through use of a template.

A. Attributable Term Template

When a new member joins the community, SecurityStarfish, LLC personnel will work with member representatives to generate an Attributable Term template of terms that may occur in an incident report and that could be used to identify a member. This template captures items like company name, facility names and aliases, IP ranges, telephone number ranges, product names and aliases, personnel names, email domains, and any other terms the member cares to incorporate into the template. This template is then used to automate removal of those terms from any incident report before it is submitted to SecurityStarfish. The template can be updated to include additional terms at any time; it is automatically applied by the member prior to submitting an incident report. With an Attributable Term template in place, the member can begin submitting anonymous incident reports to the SecurityStarfish system for distribution to the other members.

B. Incident Report Input and Anonymization

To input a report, a member's representative logs into the SecurityStarfish system on the client side. The user browses to or inputs the desired file and then moves through the selection, anonymization, review, and send steps. During anonymization, all attributable terms contained

in the Attributable Term template are excised via encryption. Excising via encryption allows the system to correlate between reports over time without identifying the actual data item. (For example, SecurityStarfish can see attacks against the same server over and over again without knowing the actual server information. It is technically possible to redact all such data, but redaction prevents invaluable comparisons over time.)

The SecurityStarfish system generates the encryption key used to excise attributable terms, but this key is held and protected by the member and never shared with SecurityStarfish servers. Therefore no attributable data ever exists in the SecurityStarfish storage system. Thus, members can recall their submitted reports from the SecurityStarfish system and decrypt the data for analysis if they so desired, but no other entity can obtain access to redacted/encrypted member data. Even if SecurityStarfish were compromised, the attacker could not attribute any data to a member since SecurityStarfish does not store any attributable data and does not know where the data came from.

C. Incident Report Content

SecurityStarfish incident report content relies generally on the Structured Threat Information eXpression ("STIX") language, an industry-standard language for describing cyber threat information in a standardized, consistent and structured manner. *See* http://stix.mitre.org/about/faqs.html#A1. STIX allows for automated sharing of indicators of adversary activity (*e.g.*, IP addresses and file hashes) and contextual information regarding threats (*e.g.*, adversary Tactics, Techniques and Procedures ("TTPs"), exploitation targets, Campaigns, and Courses of Action). *Id.* STIX is a free and open standard sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. *See id.*

D. Anonymous Submission

Once the member has reviewed the reports and is satisfied that they contain no attributable data, the member selects "send" and the files are securely and anonymously transferred to the SecurityStarfish ingest servers. Transfer of the files from the member-side appliance to SecurityStarfish servers relies on several features to ensure a completely anonymous transfer. First, the transfer occurs over an SSL channel, preventing any transfer of data in the clear. Second, the transfer occurs through a proxy service to obscure the sender's source IP address. Finally, the transfer uses the SecurityStarfish Challenge/Response authentication protocol that allows SecurityStarfish servers to identify the sender as a legitimate SecurityStarfish member without identifying that sender. The protocol utilizes a Public/Private key pair and random data to pose an encryption challenge to the sender that only a SecurityStarfish member can answer. Anonymous submission combined with attributable-term scrubbing provides for complete user control and assures the anonymity of the incident data members wish to share.

E. Report Notification and Distribution

At account setup, each member specifies email accounts and SMS numbers to be notified of new incident reports. Each time an incident report is submitted to SecurityStarfish, the report is immediately ingested and a notification sent to all authorized member accounts and designated email and SMS addresses. Ingest and notification typically takes only minutes, making for timely and up-to-date notification of new incident data. Members can access the new report either via a browser link sent with the notification or through their SecurityStarfish portal accounts. For the baseline system, all account holders can view a submitted report.

F. "Stop Light" Distribution

SecurityStarfish incident reports are distributed in a manner that does not allow for "cherry picking" certain members within an industry sector while excluding other industry sector members (such as direct competitors in a particular industry). SecurityStarfish's model assures that the incident data will be sent to all sector member peers. The sector peers as a group may decide to delay slightly informing other sectors (for example, the aviation industry might want some extra time to fix a vulnerability before the alert is shared with other non-aviation industry sectors). However, SecurityStarfish precludes the possibility of discriminating among sector peers such that some sector members would receive incident report information while others within that sector would be deprived of the same information.

G. Report Correlation and Open Source Analysis

SecurityStarfish provides account holders access to the open-source feeds and analytical tools as well as the submitted incident reports. *A priori* filters will provide quick-look indications of industry trends (*e.g.*, increasing or decreasing cyber activity in a sector or region) and statistics on types of attacks. All members will have concurrent access to the same analytical tools and incident data to enable effective joint analysis. The ability to share timely data, analysis tools and analytic results is the core capability that provides communities the efficiency and agility they need to stay inside adversaries' decision and attack cycles.

H. Collaboration Forum

A necessary feature of data sharing and joint analysis is the ability to collaborate with peers on threats and mitigation techniques. The need to ask clarifying questions and make inquiries about data and analyses are essential to sharing and developing cross-industry responses and strategies to thwart attackers. The SecurityStarfish system includes a collaboration forum for this purpose. Since anonymity is important, the forum will allow members to join the forum under an alias that does not betray their account identity. However, members are free to identify themselves within the collaboration system if they so desire. The member's level of anonymity is always under the control and at the discretion of the member, not the SecurityStarfish system.

IV. The Proposed SecurityStarfish Information Sharing System Will Not Be Anti-Competitive

The proper analytical framework for assessing the proposed SecurityStarfish information sharing system is set forth in the DoJ and FTC Antitrust Policy Statement, and a "rule of reason analysis" is appropriate here. *See* DoJ and FTC Antitrust Policy Statement at 5.

As described in Section III, and consistent with the DoJ and FTC Antitrust Policy Statement, the nature of the information shared via the proposed SecurityStarfish system is "very technical in nature" and includes the threat signature sharing contemplated by the DoJ and FTC Antitrust Policy Statement. *See* DoJ and FTC Antitrust Policy Statement at 7 ("The sharing of this type of information [threat signature information] is very different from the sharing of competitively sensitive information such as current or future prices and output or business plans which can raise concerns.").

Consistent with objectives expressed in the DoJ and FTC Antitrust Policy Statement, SecurityStarfish's "sharing of cyber threat information can improve efficiency and help secure our nation's networks of information and resources" and is "done in an effort to protect networks and the information stored on those networks, and to deter cyber attacks." *See* DoJ and FTC Antitrust Policy Statement at 6. The information sharing enabled by the proposed SecurityStarfish system is designed to provide information related to cyber attacks that each member contributor reasonably believes to be factually correct. All cyber threat information will be exchanged via anonymously-sourced incident reports that are objective and non-judgmental.

The cyber threat information shared via SecurityStarfish's incident reports is "technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plans." *See* DoJ and FTC Antitrust Policy Statement at 1. SecurityStarfish incident reports will not contain any information about member commodity or service pricing, including specific prices of any particular operating equipment, electronic information and communications systems or cyber-security systems or services, although there may be some general discussion of cost impacts of various security-related activities and program models in the Collaboration Forum. No participant's specific, competitively sensitive information about recent, current, and future prices, cost data, output levels or capacity will be exchanged directly or indirectly among participants through SecurityStarfish. *See* DoJ and FTC Antitrust Policy Statement at 4.

SecurityStarfish members will not be allowed access to confidential or non-public information about their competitor's products and services, because such information cannot be shared through SecurityStarfish's incident reporting mechanisms.

All information exchanged through SecurityStarfish will relate directly to technical and program management issues regarding cyber-security. Such information is very unlikely to provide competitors with a meaningful or competitively significant degree of cost information.

Each member will determine individually how to respond to any information exchanged and how the information will affect its cyber security (including counter-measures) decisions.

The proposed information exchanged by SecurityStarfish is not expected to affect innovation rivalry or lessen competition in the procurement of operating equipment, electronic information systems, or security-related services nor facilitate other ancillary or independent agreements that could subvert competition among manufacturers, vendors, or security services providers. The SecurityStarfish information sharing system will not be a conduit for any specific discussions or negotiations between, or on behalf of, vendors, manufacturers, or security services providers regarding any individual participant or group of participants.

V. The Proposed SecurityStarfish System Will Benefit Competition

CyberPoint and its affiliate SecurityStarfish, LLC believe that the proposed information exchange has the potential to become a unique and effective source of useful information about emerging cyber threats and countermeasures to those emerging cyber threats. Members will be better prepared to withstand and counteract the potential adverse consequences of security breaches.

The proposed SecurityStarfish system information exchange should have a pro-competitive effect to the extent that participants will be able to identify and address their security risks more efficiently, thereby reducing wasteful security-related costs (including the costs to mitigate and recover from security breaches) and allowing for more productive deployment of capital and resources. *See* DoJ and FTC Antitrust Policy Statement at 8-9 ("Indeed, to the extent that the proposed information exchanges result in more efficient means of reducing cyber security costs, and such savings redound to the benefit of consumers, the information exchanges could be procompetitive in effect.") (*quoting* Letter from Joel I. Klein, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Barbara Greenspan, Assoc. Gen. Counsel, Electric Power Research Inst. (Oct. 2, 2000), available at http://www.justice.gov/atr/public/busreview/6614.htm).

Although the exchange of information via SecurityStarfish is within and among market sectors comprised of actual or potential competitors, it is believed that the nature and substance of the SecurityStarfish information sharing (*e.g.*, via incident reports) would not increase the likelihood of collusion on matters such as price, output, or other competitively sensitive variables. *See* DoJ and FTC Antitrust Policy Statement at 6. The information shared through SecurityStarfish is less competitively sensitive and highly unlikely to lead to a lessening of competition. *See id.*

VI. Conclusion

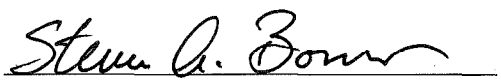
The proposed SecurityStarfish system provides an anonymous information-sharing platform and service that includes a cyber intelligence and collaboration system designed to help users quickly or even preemptively defend against cyber attacks and threats. Through

community intelligence analysis of member-provided incident and attack reports—combined with open source and SecurityStarfish intelligence analysis describing attack vectors and trends within users' regions and sectors—members would have the data and tools they would need to collaboratively identify, analyze and strategize about attacks that affect the community. Responsive and actionable intelligence allows members to recognize and respond to current attacks in their sectors and efficiently implement measures to defend against future attacks. Like the EPRI Enterprise Infrastructure Security Program analyzed by the Department in 2000, all information exchanged by the SecurityStarfish information sharing system "would relate directly to physical and cyber security, and there would be no discussion of prices for equipment or recommendations in favor of a vendor." *See* DoJ and FTC Antitrust Policy Statement at 8.

CyberPoint and its affiliate Security Starfish, LLC would be pleased to provide additional information to the Department at your request. We appreciate the Department's assistance and looks to forward your response to our request for a business review. Given government and industry's stated critical need for an effective information exchange solution, we respectfully request an expeditious review.

Sincerely yours,

FISH & RICHARDSON, P.C.



Steven A. Bowers

E-mail: bowers@fr.com
Fish & Richardson P.C.
1425 K Street, NW
11th Floor
Washington, DC 20005
Tel.: (202) 783-5070
Fax: (202) 783-2331

Counsel for CyberPoint International LLC

cc: Paul B. Kurtz, Chief Information Security Officer, CyberPoint International LLC