BlueVoyant®

Reducing Third Party Cyber Risk Across U.S. Electrical Critical Infrastructure

JUNE 2021

June 1, 2021

Michael Coe
Director, Energy Resilience
Division of the Office of Electricity,
U.S. Department of Energy,
Mailstop OE-20, Room 8G 042,
1000 Independence Avenue, SW, Washington, DC 20585
ElectricSystemEO@hq.doe.gov

Re: RFI on Ensuring the Continued Security of the United States' Critical Electric Infrastructure (6450-01-P)

Dear Mr. Coe:

BlueVoyant is pleased to present the enclosed response to your RFI released in April. Our response is centered around how our 3rd Party Cyber Risk Service (3PR) can help the Department of Energy better understand, prioritize and reduce cyber risk within the energy critical infrastructure sector, specifically requeste3d in RFI areas 1, 2 and 3. Governments and corporations around the world are using this service to manage cyber risk that results from them interacting with a growing number and variety of third parties (contractors, subcontractors, service providers, utilities, alliance partners, etc). Our solution combines unique data sources, advanced analytics, cyber expertise provided by our staff with many years of experience at NSA, FBI GCHQ and other Government organizations, and proactive mitigation management capabilities.

Thank you for allowing us this opportunity to provide our perspective. We look forward to speaking with you soon. If you have questions regarding this submission, please contact me.

V/R,

Tom Conway
Director, Federal Business Development

BlueVoyant, LLC
(703) 801.0753
tom.conway@bluevoyant

Addressing Third Party / Vendor / Supply Chain Cybersecurity Risks

Dating back at least to the Target attack in 2013 and reinforced by the more recent *NotPetya* (2017) and SolarWinds (2020) attacks, the risks of cybersecurity failures in Third Party / Vendor / Supply Chain IT have moved to the forefront of concern for company Boards, IT departments, procurement teams, and cybersecurity organizations. *CSO Online* reported in Feb 2021 that attacks on open-source software supply chain alone had increased 430%.[1] The costs of these breaches are staggering - $2 billion for Equifax, $10 billion for *NotPetya*. We see a new third party-related attack almost weekly. These attacks most often result in lost PII to theft and lost data to ransomware; but they often also result in lost intellectual property and significant disruptions to the supply chain's ability to manufacture and deliver goods / services.[2]

Year	Attack	Impact
2012	LinkedIn	165 mil records
2013	Adobe	153 mil records
2013	Target	$2 billion
2013	My Space	360 mil records
2013-14	Yahoo	3 bil records
2014	eBay	145 mil records
2016	Adult Friend Finder	412 mil records
2017	Equifax	148 mil records $10 billion
2014-18	Marriott Int'l	500 mil records
2018	My Fitness Pal	150 mil records
2020	SolarWinds	250 gov't orgs 18,000 companies
2020-21	MS Exchange	250,000 servers 37,000 orgs

100%

Of organizations have supply chains with widely varying cyber defense postures

70%

Of organizations have moderate to high dependency on external organizations

- *Deloitte 2019 Survey*

583

Average number of companies an enterprise shares confidential information with.

- *Ponemon Opus 2019 Data Risk in the Third-Party Ecosystem*

Despite the risks, digitally engaging with third parties remains a business necessity. Firms must enable various degrees of network connectivity allowing some vendors and their products access through the network perimeter. They must provide highly sensitive data (financial, PII, regulatory compliance, intellectual property, etc.) to some vendors which remains stored on the vendor networks. Firms must also interchange email with attachments, enable sharing of cloud data storage repositories, etc. All these digital connections present potential vectors for the transfer of malware and often illicit connectivity from a compromised third party to the client firm's infrastructure.

As the technologies and operational capabilities employed to defend enterprise networks have improved over the past two decades, attackers have actively sought

[1] https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

[2] https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

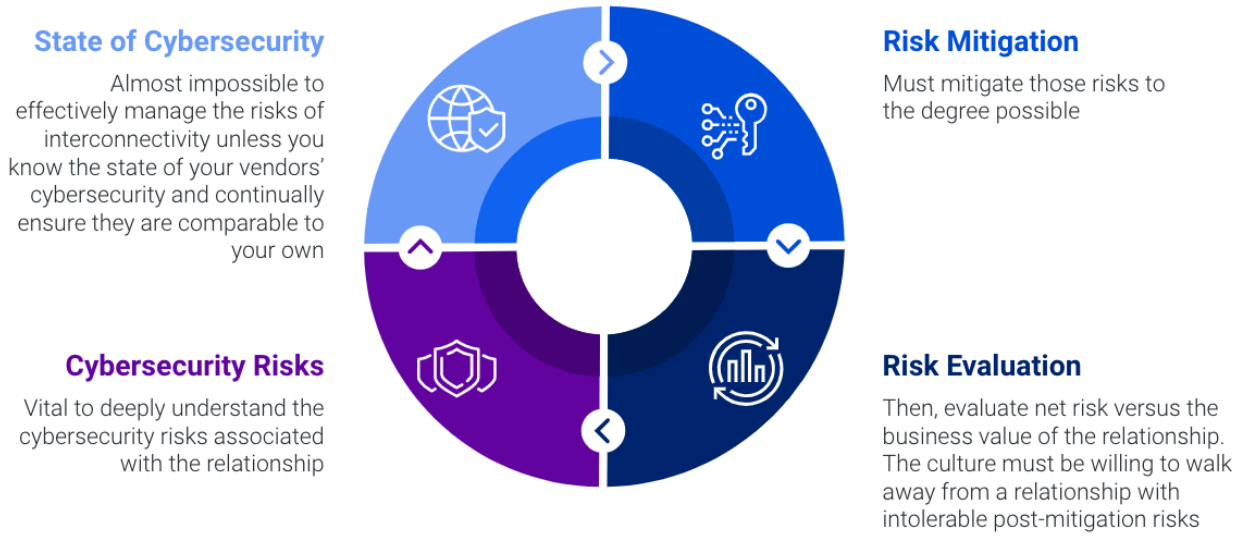
easier vectors through which to breach the perimeters of enterprise infrastructures. As much as the successful attacks mentioned above created concern for their victims, they equally attracted attackers. Consider banking institutions as an example. They are generally very secure and are heavily regulated to maintain an above average level of cybersecurity vigilance. However, the banks often outsource some functions – like bank statement production – to specialty firms. Those contracted firms are usually smaller, less regulated, and likely much less resourced; but they generally have a direct connection to the bank's accounts databases and account holder information databases. Thus, they become the easier target.

It is also worth mentioning that while many organizations have recently added rigor in their cybersecurity technologies and operations, many well-resourced and capable organizations have not. SolarWinds was not an isolated instance of a highly successful but poorly defended organization – they are far from alone. Cybersecurity is still not well understood by many corporate leaders, often not resourced properly, and in some cases, simply not a priority – even for organizations in the business of building security products.

The threat is always a valuable axis of cybersecurity risk consideration as well. Hacking today is a for-profit, international, multi-billion-dollar business undertaken by professionals – generally organized crime and nation-state funded actors. To be profitable, attackers must assess a large number of possible targets and make decisions on where to focus their attack resources for maximum impact in terms of value and volume. The most valuable intelligence is to identify organizations that are important (as a potential target) and have consistent weaknesses in their defenses. A secondary consideration is to identify normally well-defended targets that have an unexpected vulnerability – which is normally short lived. These momentary lapses are often all that a skilled hacker requires to initiate and sustain a long-term operation. Building this sort of industrial strength capability allows hackers to scale their operations, but it is technically complex, expensive, and requires sufficient depth of knowledge of offensive operations to build automated vulnerability detection engines. Most advanced cyber actors have the resources and skills to build this type of capability and have done so. The criminals collect intelligence directing them toward vulnerable targets using sophisticated tools to scan the Internet and all Internet-facing systems for vulnerabilities and general system intelligence. The efficacy of their vulnerability scanning and network intelligence collection determines their profitability – so they are getting better and better at it.

Addressing the Threat in a Comprehensive Way

It is nearly impossible to effectively manage the risks of interconnectivity unless you know the state of your vendors' cybersecurity (technically and operationally) and continually ensure they are comparable to your own. One must deeply understand the cyber risks associated with the relationship, mitigate those risks to the degree possible, and evaluate net risk versus the business value of the relationship.



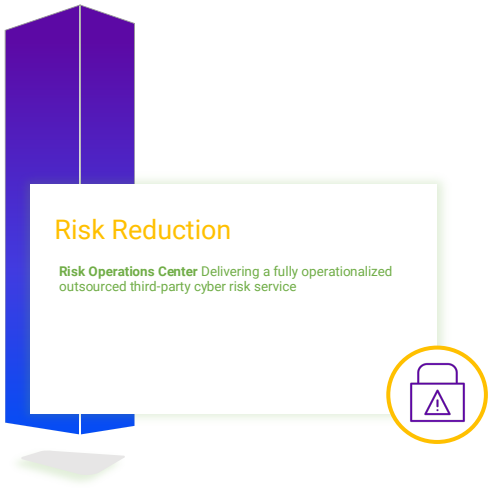
Historically, firms have used a number of techniques to assess the viability of a third party to fulfill its obligations of the contract / relationship. They assessed the vendor's financial records, production records, public records of lawsuits, industry certifications, quality, etc. These techniques evolved into a set of best practices often centered around a set of questionnaires with each questionnaire focused on some aspect of the vendor's capabilities. The firms evaluated the questionnaires and selected any concerning areas to investigate further with interviews or audits. The initial veracity and ongoing compliance of the questionnaire responses were codified in contracts, and they were periodically revisited (generally no more often than annually). As cybersecurity risks increased, firms simply followed this basic process with a questionnaire dedicated to the vendors' cybersecurity operations.

This model provided a *Risk Assessment* with some measure of visibility, assurance and risk abatement over the years; but it has not, in any significant manner, increased the cybersecurity capabilities and performance of third parties. While providing important information about the internal policies and technologies of the organization vital to understanding the vendor, the questionnaire process is simply insufficient for understanding cybersecurity risks for a number of reasons. The IT infrastructure in any enterprise changes quickly with new technologies, new manufacturing plants, new warehouses, new clouds, new apps, mergers and acquisitions, etc. Annual questionnaires cannot capture the risks resulting from this change in a timely manner.

Vendors answer questionnaires optimistically – if just one Next Generation Firewall exists anywhere in the organization, they will say they have it and allow the client to believe they are everywhere, for example. Crucially, there exists a vast difference between what most vendors think is or intend to have configured on their networks, and how their technology is actually implemented at any given moment.

Over the past decade, a number of companies have emerged providing *Risk Identification* capabilities intended to address the insufficiency of questionnaires by collecting externally available information throughout the Internet and analyzing it frequently (daily, often) to assess the current state of cybersecurity at the third party. These firms look at much of the same data attackers use to target vulnerabilities. They also employ various techniques to rank vendor cybersecurity quality and/or risk. This information can validate some of the questionnaire responses, but more often examines areas the questionnaire, by its nature, cannot contemplate. For example, the questionnaire asks – what is your patch policy (answer – "we patch monthly")? The external data can show that the vendor has browsers that have not been patched in over a year. Continuous assessment is an important step forward in providing the firm with continuously updated data upon which to make risk-based decisions.

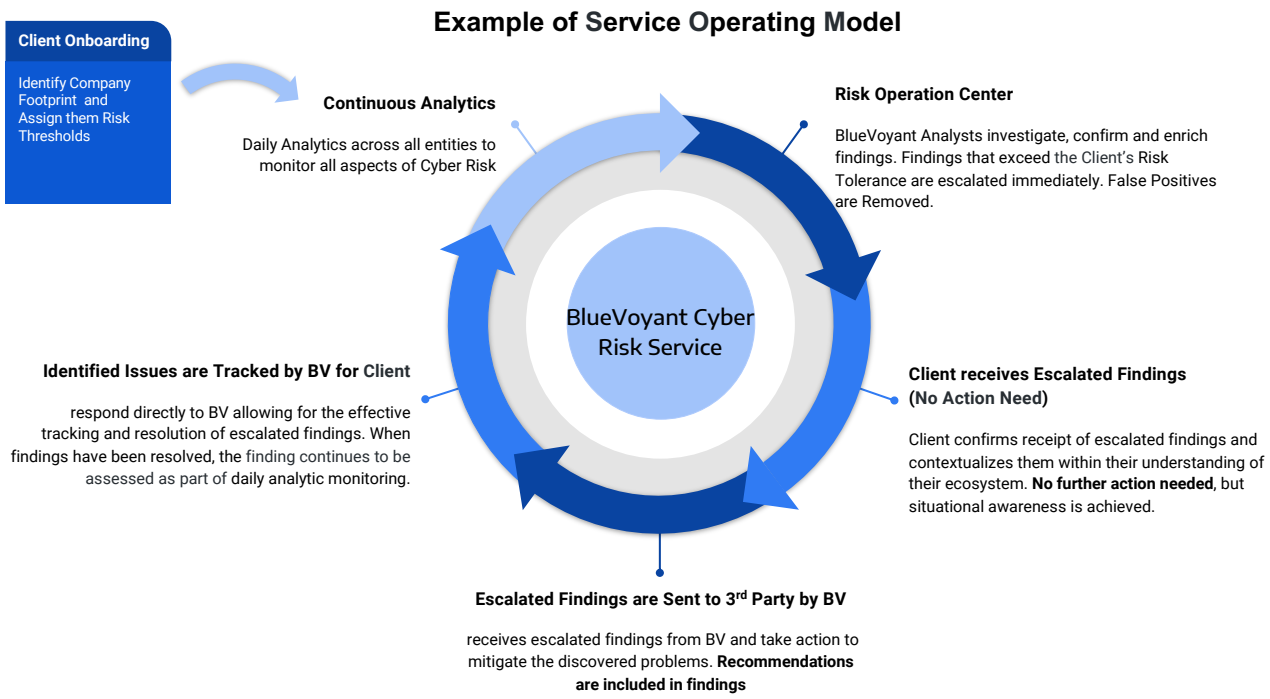
BlueVoyant provides these continuous, external assessments of almost 500,000 vendors every day. We approached the assessments differently emphasizing IT Hygiene-related metrics and vulnerability-related metrics while also including indicators of interest from threat actors and indicators of prior successful attacks. We included capabilities to mute the metrics related to certain domains or IP addresses – such as for devices that we recognize as security malware detection devices, for example. We recognized that just because a metric is measurable does not make it particularly relevant in a cybersecurity risk context, as well. Finally, we built a scoring paradigm to enable incorporation of new and emerging risk indicators / metrics without undermining the validity of historical scoring trends.



However, our hundreds of cybersecurity professionals knew from day one that in any enterprise, having actionable data and actually acting on it in the face of the tyranny of the immediate competing priorities that make up corporate IT/cybersecurity life today are very different things. It takes a tremendous amount of time, energy and focus to find the right point-of-contact at a vendor firm and subsequently work through remediations to the weaknesses identified.

To address this need for realizing actual *Risk Reduction*, we built a service modeled around the Security Operations Center (SOC) concept to not only proactively identify the risks exposed by the vendors, but also to work with vendors on the firm's behalf to accomplish remediation of those risks – to get the patches applied, to get the network ports closed, to remove the risky services, etc. BlueVoyant's Risk Operations Center (ROC) turns data into action and action into risk

reduction. In addition, we show firms the state cybersecurity risk exposure across their entire vendor portfolio as it is improving over time. We do not just make you more informed, we make you more secure.



Clients use BlueVoyant's risk service to monitor their vendors; but, critically, they also use us to assess vendors prior to formalizing the relationship – a purchase, an acquisition, a merger, etc. By doing so, we help clients put specific remediation requirements into the contracts, or price them into their acquisition/merger strategies.

The old adage of a chain being no stronger than its weakest link applies to third party risk management. BlueVoyant goes beyond identifying weak links, we help strengthen them.

1 Service Overview

BlueVoyant 3rd Party Cyber Risk Service is a managed service that reduces cyber security risks with third-party entities by continuously monitoring their security posture to ensure they meet the client's enterprise security standards and optionally engaging them on the client's behalf to resolve key security findings, providing:

- External cyber risk monitoring based upon the largest, commercially available, data sets
- Continuous external monitoring of cyber-risk and daily alerting of when a supplier exceeds previously set cyber risk tolerance levels set by the client
- The ability to externally verify and continuously monitor selected questionnaire responses
- Expert world-class, former NSA cyber attackers and defenders to review and evaluate findings and provide remediation recommendations – a curation function that allows the client to effectively focus its monitoring, evaluation, and remediation activities

A portal that allows the client to see and risk manage its whole supplier portfolio efficiently and effectively with complete transparency as to the basis for each cyber risk finding that goes into the overall risk score for each supplier

2 Service Features

2.1. Scoring and Risk Identification: BlueVoyant utilizes a combination of public and proprietary data sources, analytical strategies and machine learning algorithms to create a single risk score which is comprised of five risk categories:

2.1.1. Email Security: Identification of correct configuration and best practices for Email Security including use of spoofing and spam protection.

2.1.2. IT Hygiene: Identification of misconfigured network infrastructure and proper internal IT best practices: including exposed ports that are easily breached, administration, or unauthenticated. Additionally, detection of the internal use of peer-to-peer (P2P) file sharing and torrent software indicators lack proper IT governance and controls.

2.1.3. Vulnerability Detection: Identification of exposed vulnerabilities that could potentially be exploited including proper use of certificates.

2.1.4. Malicious Activity: Identification of malware, phishing, and ransomware emanating from the third party's environment. Detection of company's interactions with adversarial infrastructure including darknet and botnet infrastructure.

2.1.5. Adversarial Threat: Monitoring of adversarial attacks directed at the third-party company including inbound phishing and attacker infrastructure targeting the third party.

2.2. Footprinting: Identifying the digital footprint of a company, including their registered IP addresses, internet hosting presence, and external facing network assets. Footprinting is a foundational aspect of the service and is required to appropriately identify the risk posture of a company.

2.2.1. Curation & Adjustments: As part of the service, the Risk Operations Center ("ROC") will review a company's digital footprint and make adjustments if the specific company exceeds a risk tolerance.

2.2.2. Limitations: Specific companies such as telecoms, universities, hosting and cloud providers enable their customers to access the Internet as a function of their business. It can be difficult to delineate the network boundaries between the company's corporate infrastructure and their customer infrastructure and subsequently the security hygiene of the company versus their customers. Curation of the footprint of these types of companies are out of scope for the service unless the third party directly provides information on their digital footprint including external network segments.

2.3. Data Collection: The data collected by BlueVoyant from the client will be the contact information for risk managers at both the client and their various entities. The required information will include full name, email address, phone number, and street address of primary business location.

2.4. Risk Tolerance: During the onboarding process, a "risk appetite" is created by grouping companies into portfolios and defining risk criteria. When a company exceeds a risk tolerance as defined by the risk tolerances, the company and applicable findings will be queued to the ROC for review and confirmation. Risk tolerances are an important aspect of the service to balance risk to the client and

the operational costs and resources to engage the client and third-party companies on minor security findings across their third-party entities.

2.5. Playbooks and Automation: Playbooks and automation represent a key part of the service to enable appropriate service scale. When a finding is detected playbook automation will automatically trigger to perform additional analytics to both confirm the finding or provide further context to better understand the nature of the finding.

2.5.1. Noteworthy Playbook: Security Device Identification: The security device identification playbook is focused on analyzing entities devices that exhibit a high volume of malicious activity over a specific period of time, such as a work week. The playbook detects the presence of security devices based on their behavioral traits and enables the risk alerts that would typically be generated by those devices to be appropriately muted to avoid confusion and time consumption on the part of the ROC, the client, or entities. The playbooks make it possible for BlueVoyant to scale this service to many entities simultaneously.

2.6. Client Notification and Escalations: When a company exceeds a risk tolerance and the finding has been reviewed and confirmed by the ROC, the client's point of contact will receive an email notification.

2.7. Portfolio-Wide Vulnerability Alerts: When major vulnerabilities are announced publicly by leading government cybersecurity agencies BlueVoyant develops applicable vulnerability detection analytics and apply them to the entire portfolio to provide immediate alerts for the Client and 3rd parties. Moreover, BlueVoyant will positively confirm that the vulnerability is not present in the 3rd party ecosystems if it is not present.

2.8. First Party (Client) Risk Assessment: As part of the service, the client company will be monitored in the same manner as a third-party company is monitored.

3 Supporting Features and Teams

3.1. Risk Operations Center ("ROC"): The ROC is a team of cyber risk analysts attached to the BlueVoyant Security Operations Center (SOC) responsible for the triage,

analysis, escalation and tracking of risks in the entities ecosystem that exceed the client's risk tolerance.

3.2. BlueVoyant Client Portal: The BlueVoyant Client Portal is a web-based portal that provides real-time visibility to findings, reviewed findings, enables communication with the ROC (approved client employees), view the security posture of the client's company and their identified third-party companies.

3.3. **Reporting:** The BlueVoyant Client Portal features report generation on demand for all findings or escalated findings based on client preference.

3.4. **BlueVoyant 3rd Party Portal:** The 3rd party portal allows each individual 3rd party to view their current findings and respond with their intentions to resolve the findings. This feedback is automatically queued to the ROC for assessment and follow-on actions.

3.5. BlueVoyant Risk API: The BlueVoyant Risk Application Programmers Interface (API) provides programmatic access to the data elements visible in the portal enabling integration with ticketing systems, global risk and compliance tools, security information and event management system, and other platforms where appropriate.

4 Client Onboarding:

4.1. List of Companies/Suppliers: The client will provide the list of companies that will be monitored for as part of the service. In order to monitor the correctly identified company the client will provide both the *company name* and *primary domain* in order to disambiguate from other companies with similar names or brands.

4.2. Portfolios: Portfolios are a method to group companies together for easier management, typically for risk tolerances. When the client provides the list of companies as part of onboarding, they will also provide the list of portfolios and the mapping of what companies belong to which portfolio. Some common criteria for grouping companies into portfolios, but not limited to:

4.2.1. Relationship: Portfolios can be organized by the relationship of the client with the third party; for example: payment processor, supplier, distribution partner, subsidiary, etc.

4.2.2. Network Access: Companies that have direct access and the scope of access to the client's computer systems. If a third-party exhibits indicators of a breach and whether a threat could move laterally to the client's environment.

4.2.3. Data & Compliance: What type of data does the third party have and how does it relate to the client's compliance requirements?

4.2.4. Business Disruption: If the third party suffered a serious security incident or breach that disrupted operations, how impactful would it be to the client's business operations.

4.3. Risk tolerances: During the onboarding process, the ROC will work with the client to specify risk tolerances for each of the portfolios created. Definition of risk tolerances are quite flexible and can include, but are not limited to, tolerances set by overall company score, category score, specific finding type, degree of score impact, finding severity, as well as other criteria. The BlueVoyant Customer Success team will provide recommended risk tolerances at the time of onboarding.

4.4. Engagement Policy: The service can be tailored per the client's request on when to directly engage a third party when a risk tolerance is exceeded:

4.4.1. Escalation Only: If a risk tolerance is exceeded, the ROC will only alert the client and not take any direct action with the third party. This is the default state of the service for all entities during the onboarding stage of the service.

4.4.2. Per Engagement: If a company exceeds a risk tolerance, the ROC has permission to directly engage the entities, but will need to obtain prior approval from the client before engagement.

4.4.3. Pre-Approved Engagement: If a company exceeds a risk tolerance, the ROC will notify the client, but will also engage the third party directly to resolve their security findings.

4.5. Point-of-Contact: The client will provide email and phone information for the primary escalation point-of-contact as well as the primary owner of the client third party risk program.

5 Service Level Agreements

5.1. Third Party Monitoring: The Client shall receive a communication (according to the escalation procedures defined or in the manner pre-selected in writing by Client, either through the Portal, email, or by telephone) to findings that exceed risk tolerances for third parties once a review of the finding has been completed. Findings review is measured by the time that an analyst has completed their investigation in order to prevent notification for benign or false positive alerts.

5.2. Escalation Governance: Clients can set risk tolerance thresholds according to risk appetites to identify third-party companies that need to mitigate security findings to reduce their implicit risk to the client's organization. For any third-party that is under active escalation, the BlueVoyant Risk Operations Center will investigate findings, provide tailored recommendations, escalate to the client, engage the third-party, adjust footprints, and provide general support to facilitate the third-party to resolve their findings.

.

6 Client Communications: Below are the standard methods that the Service enables for the client to obtain information related to the Service or engage BlueVoyant staff.

6.1. Customer Success Manager Engagement: BlueVoyant will assign a customer success manager for the Client to provide monthly and quarterly performance reviews.

6.2. BlueVoyant Customer Portal: The BlueVoyant Customer Portal is the primary method for clients to stay informed of security activity in their environment and activities of the BlueVoyant Risk Operations Center. At any time, a client may go to the BlueVoyant Customer Portal and review findings, dashboards, or reports.

6.3. BlueVoyant 3rd Party Portal: The BlueVoyant Customer 3rd Party Portal provides direct access to the relevant findings identified by BlueVoyant for a specific 3rd party. This portal also allows for the tracking of the responses from the 3rd party and provides for a direct feedback loop with the ROC and the 3rd party.

6.4. Email: The client will receive emails as a regular function of the Service. Email topics can span a wide variety of matters, but most often they relate to findings review and confirmation investigations: notification of risk or questions on appropriate environment use or behaviors.
Clients can also initiate service change requests via Email by sending an Email to: riskservice@bluevoyant.com. Upon receipt of any emails, a service request case is created and can be viewed within the BlueVoyant Client Portal.

6.5. Calling Risk Operations: The BlueVoyant Risk Operations Center (ROC) is available 24 / 7 / 365 days a year and can be reached by calling US Toll-Free: 1-888-602-2007. Only approved client employees will be allowed to talk with BlueVoyant Risk Operations and will be authenticated when their call is received.

7 Third Party Engagement: As part of the Service, BlueVoyant can, subject to paragraph 1,3 above, directly engage the client's entities to encourage resolution of findings, provide supporting evidence, adjust third party footprints, answer questions, and track resolution commitments. When and how BlueVoyant engages the client's third party can be tailored to the client's needs.

7.1. Client Support: The client will provide a third-party point of contact as a prerequisite to enable BlueVoyant to engage the third party, subject to the engagement model the client has specified. The client may be required to be involved in third party communications in order to establish BlueVoyant as a representative of the client. Additionally, the client may need to exert influence on the third party to resolve specific findings if the third party is unresponsive.

7.2. Interaction Methods:

7.2.1. Email: The primary method of communication with a third party is through email. An introductory email would be sent once a third party has exceeded risk thresholds, either by the client or from BlueVoyant with the client carbon copied.

7.2.2. Phone/Video Conferencing: BlueVoyant will leverage video conferencing technology to discuss findings with third parties.

7.3. Responsiveness: Third parties will be denoted as responsive, unresponsive, or not engaged within the BlueVoyant platform depending on their level of engagement After multiple attempts of engagement with a third party BlueVoyant will mark a third party as unresponsive within the platform.

8 Client Responsibilities: The client's responsiveness and engagement will drive the onboarding process, the insertion of entities into portfolios, the setting of risk tolerances and the engagement policy for the entities in their ecosystem. All of these steps must be successfully completed, to activate the service. Completing only a subset of these activities will result in BlueVoyant being unable to activate the service.

8.1. Onboarding

8.1.1. List of Companies/Suppliers: In order for the engagement to begin in earnest, the client must provide a list of companies (also called entities). The onboarding process cannot proceed without this being properly completed, and delays in this process will delay the implementation of the service.

8.1.2. Portfolios: The assignment of entities to portfolios is a necessary step in order to group like entities together as they have similar risk profiles and tolerances. By placing them into smaller portfolio groups, BlueVoyant can treat them appropriately and prioritize follow-on actions accordingly.

8.1.3. Risk Tolerances: Risk tolerances must be set to ensure the appropriate subset of risk findings is raised to the Client regarding the entity's ecosystem on a day-to-day basis. Setting appropriate risk tolerances based on the risk profile of the groups of entities in each portfolio is the logical way to ensure the priority of each entities is taken into account when raising cyber risks for action.

8.2. Third Party Engagement: When the ROC has been delegated the authority to represent the client to the third-party entities, the ROC will proceed to contact the entities with the details of the cyber risk findings, along with the supporting data necessary for the entities to determine the nature of the cyber risk. The ROC will also make a recommendation on how to address the cyber risk and resolve the cyber risk finding. The ROC will interact directly with the entities in this scenario. The client will have insight via the BlueVoyant portal and may also request to be included in any communication with the entities at any time.

8.2.1. Third Party Point-of-Contact: The client must provide complete third-party entities contact information to include the full name of the entity's IT or security representative, the email address, phone number, and business location address of the entities' headquarters.

9 Additional Service Terms and Conditions:

9.1. Resolution of Findings: Resolution of Findings is dependent on third party company engagement and commitments from the third party. BlueVoyant is not held accountable to the promises of third parties and cannot guarantee that third parties will engage, respond, and resolve identified security findings.

BLUEVOYANT DIFFERENTIATORS

Value Proposition

BlueVoyant uses the skills of former government cyber experts to build easy target identification capabilities similar to those employed by nation states and advanced criminal groups, but deployed for defensive purposes. Our mission is to provide an external layer of cyber protection to the US CI/KR sectors in order to significantly reduce the number of soft targets available to adversaries.

BlueVoyant is able to do this because of five core capabilities:

Scale and Speed - BlueVoyant can generate and enrich cyber risk findings on all USG chosen institutions on a daily basis and can evaluate escalated findings (e.g., Microsoft exchange) in less than one hour.

Accuracy - Two keys to accuracy. First, getting the internet-facing footprint of domains and IP addresses right for the financial institution. BlueVoyant is able to do so by leveraging its very large real-time DNS dataset in addition to registration data. Second, eliminating false positive findings emanating from guest networks and security devices utilizing automated algorithms.

Proprietary and commercial datasets. BlueVoyant has exclusive commercial rights to a number of important datasets including real-time data, and also uses a number of commercially available datasets.

Expert curation of findings. All vulnerability and compromise findings are reviewed for accuracy, importance, and remediation instructions by cyber experts in BlueVoyant's Risk Operations Center.

Operationalize with automated support remediation. BlueVoyant is focused on actual protection by eliminating externally visible material cyber risks. This involves curating findings down to the important manageable core and following up with at risk institutions with remediation guidance.

Ease of implementation. BlueVoyant does not require the installation of any device or software at the financial institution nor require any data to onboard a financial institution other than the name, main domain of the institution.

This capability will enable USG to do each of and all of the following:

- View the externally visible cyber risk posture of every U.S. CI/KR institution daily and see which have serious cyber vulnerabilities visible to cyber attackers (or external evidence of compromise) and which ones do not.

- View progress over time in eliminating soft targets CI/KR sectors.

- Have BlueVoyant either directly, or through a USG approved intermediary, provide those institutions with details on serious vulnerabilities or evidence of compromise with instructions on how to operationalize the handful of specific remediations needed.

- When an externally visible new vulnerability arises (e.g., SolarWinds, Microsoft Exchange, F5), alert all impacted financial institutions within hours through BlueVoyant or a USG approved intermediary.

- Identify those organizations creating ongoing systemic risk within and/or across sectors by their repeated or persistent failure to maintain appropriate externally facing cyber defense.