North American Transmission FORUM

Community Confidentiality Candor Commitment

NATF Industry Collaboration: Using Solution Providers for Third-Party Risk Management

Version 1.0
Document ID: 1576
Approval Date: 09/17/2021

Versioning and Acknowledgments

Version History

Date	Version	Notes
09/17/2021	1.0	Initial Document

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Acknowledgments

This guide was developed by supplier and solution provider members of the Industry Organizations Team:

Fortress Information Security
GE Grid Software Solutions
Hitachi-ABB Power Grids
Hubbell Incorporated
KY3P HIS Markit
Nebraska Public Power District (NPPD)
Schneider Electric
Schweitzer Engineering (SEL)
Siemens Industry, Inc.
UL

Contents

1. Solution Provider Guide Objective

The objective of this document is to provide a guide for entities who choose to work with solution providers to receive the benefits of the solution providers' services while managing potential supply chain risk.

Entities are increasing their supply chain security risk management efforts and in many cases are turning to third-party companies (herein referred to as "solution providers") to assist with these efforts.

In light of the evolving cyber security risk landscape and regulatory developments, entities are growing more cognizant of cyber risks that can be introduced through their supply chain. Their awareness and concern are heightened by new regulations, including the NERC supply chain standards,[1] which initially became effective on October 1, 2020, and are revised from time to time,[2] as well as the United States Executive Orders and related requests for information and prohibition orders.[3]

Solution providers can assist with an entity's supply chain risk assessment and mitigation by offering a variety of services, including providing assessments to evaluate suppliers' security practices and helping entities implement ongoing supplier security risk management. *In providing these services and benefits, solution providers become part of the entity's supply chain and, as such, should also be assessed for potential risks.*

One way a solution provider can conduct an assessment is to use the NATF Supply Chain Security Assessment Model ("NATF Model"). The NATF and industry organizations have worked together to produce the NATF Model and tools to address supply chain cyber security risk assessment. The NATF and the Industry Organization Team, consisting of electric utilities, energy industry trade and forum representatives, suppliers, third-party assessors, and solution providers,[4] have provided the NATF Criteria[5] and NATF Questionnaire[6] that entities can use to evaluate supplier cyber security practices. The NATF Criteria are mapped to security frameworks that entities can look to for accuracy of suppliers' responses and assurance of suppliers' adherence to relevant criteria. Additionally, the Industry Organizations Team provides complimentary tools to assist with risk assessments, purchase agreements, and more.

This document provides a guide for items to consider when employing a solution provider, including the scope and benefits of services, how the solution provider engages with suppliers and with their customers (entities), and the solution provider's security.

---

[1] In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed new Reliability Standard CIP-013-1 and modified Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards."

[2] Information on the most current version of the supply chain standards can be located on the NERC website: https://www.nerc.com/Pages/default.aspx.

[3] Information on the status of the US executive orders: https://www.energy.gov/oe/securing-united-states-bulk-power-system-executive-order.

[4] Information available on the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[5] The NATF Supply Chain Security Criteria for Suppliers (NATF Criteria), available on the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[6] The Energy Sector Supply Chain Risk Questionnaire (Questionnaire), available in formatted and unformatted versions on the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

2. Definitions

The definitions provided below are the definitions for terms as used in this document.

Entity

An organization or company that either owns or operates bulk-power system assets.

NATF Criteria

The NATF Supply Chain Security Criteria, established by NATF members, solution providers, suppliers, and assessors, can be used to evaluate the cyber security maturity of an entity's suppliers and risk associated with their offers and services.

NATF Questionnaire

The Energy Sector Supply Chain Risk Questionnaire (Questionnaire) provides questions developed by NATF members, solution providers, suppliers, and assessors that can be used to obtain information regarding a supplier's cyber security practices.

Solution Provider

Companies or organizations that provide products or services to assist with an entity's risk assessments for suppliers. A solution provider offers a variety of services to an entity or supplier. These may include providing assessments to evaluate cyber security practices and help entities implement ongoing supplier security risk management.

Supplier

Companies providing goods, services, or data to an entity.

3. Solution Provider Assessment Benefits

There are many benefits to taking advantage of a solution provider's services.

Solution providers can assist an entity by performing resource-intensive research and analysis to streamline supply chain security assessments. Solution providers can:

- Assess the security postures of multiple suppliers
- Identify security issues a supplier may need to mitigate to achieve a desired, expected, or required security level
- Provide a simple, yet meaningful result, score, or level for each assessment
- Enable each supplier to reuse the same assessment result for multiple entities to optimize the effort and cost involved with the assessment

Solution providers can provide an independent perspective, confidential information sharing, and use of a consistent methodology across multiple suppliers and over time. Solution providers may recognize existing industry security certifications, standards, and frameworks; collect evidence from suppliers; and consider publicly available information to show suppliers' adherence to criteria. The assessments conducted by solution providers will utilize the relevant certifications to security frameworks from qualified auditors, evidence received through supplier collaboration, and public information as well as the solution provider's independent review.

Solution providers, as a good practice, may refresh supplier assessments on an annual basis and should not consider assessments and certification results to be valid for longer than 15 months. Entities can consider whether the solution provider's re-assessment and review timeframe aligns with the entity's NERC CIP-013 supply chain risk management timeline. In addition to reviewing the assessment for the supplier, solution providers may assess a supplier's product and system security practices, such as regular vulnerability scanning and software update or patch validation. A solution provider's review may be augmented with data analytics for risk management, leveraging data from a variety of public information sources. Data analytics can be available as a point-in-time or part of a continuous monitoring service.

As part of supplier assessments, suppliers can provide digital, hardware or software bills of material (DBOM, SBOM and HBOM), declare the origin (such as countries where development environments and personnel are located), foreign ownership, control, or influence (FOCI), and movements (shipping logistics) of

Solution Provider Assessment Benefits

- Helps suppliers and entities better understand gaps in suppliers' security posture and identify risks for mitigation
- Helps implement and strengthen cyber security risk management and continuous improvement plans
- Helps eliminate redundancies across suppliers and entities, including individual divisions and business units, as part of cross-functional procurement and cyber security risk management processes
- Helps reduce suppliers' workload by providing results to multiple entities
- Helps differentiate a supplier's security posture
- Helps objectively demonstrate security to multiple entities or groups of stakeholders
- Provides security for supplier confidential information by monitoring the levels and amount of information securely provided to entity
- Provides consistent assessments over time and across suppliers

products and components to establish product or component provenance.[7] Suppliers can include this information for their own supply chains as well.

Overall, what is critical for supply chain security risk management is to apply a risk-based approach to consider supply chain partners' and systems' risks, whether risks can be mitigated, and to determine the necessary levels of security and associated policies, controls, and criteria for partners, services, systems, and products.

For potential purchase decisions that have been identified as a priority in the entity's risk-based approach, a solution provider can assist by providing:

- a ***holistic*** and ***comprehensive*** view of potential suppliers' security posture (e.g., across information management and product development practices[8]), and
- an evaluation for potential suppliers' security postures using fair and consistent, or ***uniform***, assessments of the security posture from supplier to supplier and over time.

Solution providers using the above approach can provide entities with ***meaningful insight*** for security risk management planning, decisioning and actions, and allows suppliers to use assessment results with multiple entities.

4. Scope of Solution Provider Assessments and Services

Solution providers offer different services; entities should verify what services are offered by the solution provider to ensure it aligns with the organization's needs.

Solution providers generally offer the following services to help mitigate supply chain risks:

- Supplier Controls Assessments
- Central Repositories of Attestations
- Data Analytics-Based Assessments
- Digital, Software, or Hardware Bill of Materials Analysis

Types of Assessments and Services Offered

- Supplier Controls Assessments
- Repository of Attestations
- Data Analytics Assessments
- Bill of Materials Analysis

The different types of services are explained below. These services are not mutually exclusive, as entities may select a combination of services or, depending upon the solution provider, elements of the services. Each may provide different value and different levels of assurance. Entities can inquire as to the type of service a solution provider is using and how that meets their risk and assurance needs.

[7] Product or component provenance is there to determine point-of-origin and if this poses any risk. Criteria can outline security labeling techniques to help as well. An example of a framework to base criteria on is IEC 20243-1 for integrity of hardware and software products through the product lifecycle to mitigate risks of tainted and counterfeit products.

[8] For example, ISO 27001 focuses on the information security management system of the organization, ISO 22301 addresses business continuity management, IEC 62443-4-1 addresses the secure development processes for software and hardware components, products and systems, or IEC 62443-3 and IEC 62443-4-2 address security requirements for industrial automation and control systems and products, at system and product level.

Supplier Controls Assessments

Solution providers typically perform supplier controls assessments with supplier involvement. These assessments are comprised of the solution provider collecting information from a supplier using a survey-based questionnaire and collecting or reviewing supporting evidence. Evidence may be in the form of policy or procedure documentation and may include another independent third-party assessment or certification to a published security standard or framework.[9] This helps to substantiate the answers to the survey. Once the supplier has provided their answers and evidence, subject to confidentiality provisions, most survey-based assessments require 2-10 weeks to complete, depending on the size and complexity of the supplier being evaluated. However, suppliers using the NATF Criteria or Questionnaire may have responses already prepared and readily available.

The NATF Criteria or Questionnaire can form the basis for supplier controls assessments. The use of the NATF Criteria and Questionnaire increases the effectiveness and efficiency of risk assessments by reducing duplication and supporting supplier responses. The NATF Criteria and the questions in the Questionnaire have been developed with collaboration and input from across industry and represent key information that entities need when identifying potential risks. A solution provider may obtain information using the NATF Criteria or Questionnaire or may include these criteria or questions in a larger questionnaire. However, an entity should be aware of whether a solution provider obtains information or responses to all of the criteria and questions. In an instance where a solution provider does not obtain, or attempt to obtain, all of the information, an entity should be aware of what information is not collected and why.

Central Repositories of Attestations

Solution providers often request attestations to certain performance metrics or industry standards from suppliers in lieu of evidence. As such, solution providers serve as a central repository for multiple supplier attestations. The attestations are often supported by supplier statements that ensure the validity and accuracy of the information provided. The attestations may also be supported by some evidence in addition to the statements, however while the attestations, statements, and evidence may be ***reviewed***, they are often not ***validated*** by entities or solution providers. Where validated assessments are needed, an entity may want to request additional sources of information and assessment.

Data Analytics-Based Assessments

Many solution providers deliver assessments via a data analytics option that can be used to either supplement or replace traditional questionnaires or controls assessments. This form of assessment does not necessarily require the involvement of the supplier, or even their awareness. There is a growing amount of publicly available information which can be gathered by the solution provider through automated tools to provide snapshots of supplier information. Information on a supplier's financial health, cyber security ratings, vulnerability disclosures, global points of presence, and other pertinent information may be accessible via public records. Often these assessments are completed quickly and available to the entity a few hours or days. In addition, these assessments can be performed in a continuous manner to provide rapid updates. However, when using this approach, careful attention should be given to the validity of such public information. An entity

[9] Such as a SOC 2 Type 2, SOC for Supply Chain, ISO 27001, or IEC 62443.

may wish to contact the supplier, directly or through a solution provider, for an explanation of identified risks. Entities can consider:

- *Scope* - Can an external view of a conglomerate supplier accurately represent the various divisions within the supplier that are serving the entity?
- *Correlation does not imply causation* - The "public presence" (e.g., security settings on a supplier's website) is often NOT maintained by the same personnel developing or supporting the product being sold to the entity. Whether such security settings are good or poor does not necessarily reflect the security and quality of the product line for the product the entity is purchasing for use on the bulk power system.
- *Source* - Were the sources from "official" sources only (e.g., the supplier's website) or does it include "unofficial" sources, such as a professional networking platform or media reporting?
- *Timeliness* - Could the assessment rely on information in the public domain that is out-of-date? Just because something bears a supplier's name does not mean the same supplier still owns the division, as the brand may be transferred for brand-recognition purposes.
- *Completeness* - Is the data telling 100% of the story, or only 10% due to the information that was located publicly?

Digital, Software, or Hardware Bill of Materials

Often referred to as a DBOM, SBOM or HBOM, bill of material (BOM) assessments provide important information about the software or hardware components of systems the entity may purchase. This analysis requires the supplier to provide BOMs for the product, or the solution provider may perform the assessment independently in coordination with the entity. The BOM data, to the degree that it is available, is often combined with other data analytics, supplier controls assessments, or attestations to provide additional insight about the BOM components such as fourth-party suppliers, foreign ownership, or influence (FOCI), or vulnerability disclosures.

5. Solution Provider Engagement Options

Understanding a solution provider's engagement practices with suppliers and its customers (entities) is important.

Supplier Engagement Activities with Solution Providers

Managing disclosures

It is important for all parties involved (the entity, solution provider, and supplier) to understand how information obtained by the solution provider will be managed and shared.

While an entity and a supplier are likely to already have established confidentiality provisions due to a product purchase, this would not be true between the supplier and a solution provider, or a solution provider and its customer (an entity), at the outset. Not unlike the entity's use of questionnaires and contractual terms and conditions (T&Cs) to assess or obtain risk information from their suppliers, suppliers will likely require the same of the solution provider before entrusting them with their confidential data. Similarly, T&Cs need to govern sharing of data between the solution provider and its customers (entities). When engaging a solution provider,

entities should understand how the solution provider is assessing and managing supplier data, and be prepared to help their supplier obtain the following information and T&Cs from the solution provider:

Confidentiality of supplier's answers / evidence

Where is the information stored? How is it protected? Who has access on the back end and how is access controlled?

Who can request access to a supplier's questionnaire/evidence: Any of the solution provider's customers (entities)? Competitors? Regulators? Only entities the supplier confirms as customers and authorizes? When and how is that enforced?

Integrity of supplier's answers / evidence

Does the solution provider verify that answers/evidence provided at the time a supplier answers the questionnaire are true and accurate? How do a supplier and a solution provider verify the supplier's information remains accurate over time?

How does the entity, the supplier, and the solution provider ensure that the supplier's answers/evidence have not been maliciously or accidentally altered before being provided to an entity?

Governance of the answers and materials provided

What is the solution provider allowed to do with the information a supplier provides? Some solution provider's "supplier agreements" are presented as a "click through" that would grant the solution provider excessive rights regarding the supplier's information, such as sublicensing and creation of derivative works.

Responding to security incidents occurring at solution providers

How are suppliers notified if and/or when there is a security incident at the solution provider that involves the supplier's data? Which party, the entity or the solution provider, is liable to the supplier in the event of such a breach, and is the liability financial or nonfinancial?

Proprietary supplier information – supplier provided versus shared evidence

Knowing how the solution provider protects supplier information it receives is another indication of a solution provider's security practices. It should be standard practice for supplier information to remain the property of the supplier and be protected using agreed-upon mechanisms, similar to an entity's bulk-electric system ("BES") cyber system information ("BCSI"). Often, a supplier will share the agreed-upon information with the solution provider via the solution provider's portal or offline using a screen share or onsite visit, which the solution provider will document as evidence reviewed. Importantly, it is beneficial to know the solution provider's practices for reviewing the evidence, the controls they have in place to ensure reviews are done consistently, and what is documented from the review.

Refreshing supplier information – periodicity

Given that the NERC supply chain standards and related regulations are subject to oversight and enforcement, how long an assessment or certification is considered valid, or up to date, is of concern. A solution provider typically defines how often it refreshes a supplier assessment. An entity and the suppliers should be aware of the solution provider's policy and if the solution provider is able to provide flexibility - such as for more frequent

refreshes of assessments. For instance, if a NERC registered entity is audited once every three years and the supply chain standards require an annual review of policy and procedures, an entity will need to know when periodic updates to solution provider assessments are conducted. While there are no regulated practices for how long a supplier assessment is valid, and the need to refresh assessments is dependent upon the risk of the supplier and product, some recommendations to consider include:

Every 15 months for critical infrastructure

For critical infrastructure, as determined by the entity, consider requesting an updated assessment of suppliers that play vital roles in protecting or operating the related technologies or services on an annual basis or every 15 months. It is not unusual for an entity to review key aspects of their business from an internal or external audit perspective annually and, given certain asset and process criticality, the related suppliers should be addressed in a similar manner.

If the entity is planning for a major purchase of critical infrastructure, it should consider whether a refresh of the solution provider assessment is necessary.

Change to a supplier's control environment

If the supplier has undergone a change in its internal control environment or is involved in a merger or acquisition that affects its control environment, a refreshed assessment may be requested to determine if the controls or control environment has changed and requires additional review. Solution providers may or may not know about such a change. An entity may want to determine what agreements or contractual terms they have, or the solution provider has, with suppliers for providing information regarding updates or changes. In addition to mergers or acquisitions, addressed control environment changes may include, for example, a major security compromise or breach, or a change in manufacturing locations to or within a country of concern.

Associated costs

The more frequent the assessment is refreshed, the greater the increases in cost, due to the additional time demands on all parties stemming from activities such as:

- The supplier updating their answers in the solution provider's portal and/or hosting the on-site assessments
- The solution provider reviewing supplier's changes and visiting suppliers
- The entity reviewing the solution provider's updated assessments and output

Understanding the requesting organization

It is the supplier's choice, based on its risk appetite, to share its responses broadly or only with specific authenticated customers. This is typically established within a supplier's procedure and implemented with controls. At a minimum, a supplier will want to understand who is the requesting the information and how it would be used.

Approving the results – supplier involvement and validation of results

Entities and suppliers may benefit from knowing if the solution provider offers suppliers an opportunity to review a draft assessment report before it is shared in order for the supplier to challenge and correct any inaccuracies. Similarly, an entity and a supplier should be aware of whether it is the solution provider's practice to obtain a supplier's permission to share a completed report with additional customer(s) each time a request is made unless alternative arrangements are made.

Customer Engagement Activities with Solution Providers

Managing supplier requests and questionnaires

Solution providers vary in how much they permit their customers (entities), to be involved during the assessment process. Most solution providers offer their customers the ability to manage end-to-end workflow of questionnaires and assessment requests throughout the full life cycle: from initiation, through escalations, and finally to post-assessment follow-ups. Some solution providers have this capability available on a modular basis as either a standalone service or as part of a broader third-party risk management (TPRM) solution.

Using solution providers' evidence repositories (i.e., repurchase)

Some solution providers have an inventory of previously completed assessments that can be requested for purchase – this is known as a "repurchase." In those cases, as discussed above, it is important to know if the solution provider is required to seek permission from a supplier before granting access. It would also be important to know when the assessment was conducted – i.e., how "old" it is – and if the repurchase includes any continuous monitoring or if the assessment is periodically refreshed. Entities should also consider the following when determining whether to use the solution providers' evidence repositories.

Who conducts assessments

The entity

In cases where information is gathered in the form of a questionnaire with supplemental uploaded evidence, an entity may want to control the assessment and have solution providers, which may include assessors and/or risk partners, review the provided information pursuant to the entity's risk policies. This approach may need to be approved by the supplier, as the entity's T&Cs with the supplier may prohibit the entity from sharing supplier's information with another solution provider without the supplier's express written consent. There may be benefit in this approach for suppliers, as both the entity and the solution provider can have direct communication with the supplier to request any additional clarifications and share findings for discussions regarding mitigation or risk acceptance.

The solution provider

Solution providers develop their validation methodology based on the assessment types that they offer. Assessment types range from a deep onsite assessment to a "low-touch" documents and controls review. Information is typically requested in the form of a documents request list and/or questionnaire.

It is important to know the qualifications of the solution provider personnel performing the assessment. Qualified auditors are trained to perform assessments methodically and consistently, ensuring that assessments of different suppliers can be compared. Solution providers typically have qualified assessors with relevant domain experience and/or certifications on staff and, depending upon the size of the organization, may have global teams.

However, even when a solution provider conducts the assessment, it remains the responsibility of an entity that consumes an assessment report to understand the scope and findings and make risk-based decisions to accept a risk or request remediation of identified risks. A solution provider should expect that an entity may follow up with additional questions or clarification requests.

How to use results

Controls assessments

It is important for an entity to understand the findings of an assessment, the solution provider's opinion on the severity of each identified risk, and the degree to which the supplier's compensating controls will mitigate the risk. Each entity needs to make their own risk-based decisions to accept or remediate findings based on the compensating controls in place and risk appetite. Some solution providers offer extensive details in their observation statements and access to select underlying evidence (with supplier permission).

3rd-party certifications

A solution provider practice for a controls assessment is to leverage independent control attestations, such as a SOC 2, SOC 2 Type 2 or SOC for Supply Chain,[10] or relevant certifications, such as ISO or IEC[11]. Depending upon the scope of the assessment, these independent control reports or certifications may validate a portion of the controls assessment, but often solution providers must supplement these reports or certifications with further evidence. It is important for entities to understand how a solution provider leverages the reports or certifications (time, scope of the right service, any qualified opinions, etc.) and documents their process.

Data analytics

In addition to the controls assessments, some solution providers augment reports with data analytics from additional sources such as cyber security ratings, financial health, negative news, open-source intelligence, data breach history, location risk, etc. The data analytics can be available as a point-in-time or part of a continuous monitoring service.

Some solution providers offer data analytics as is, or with ability to further engage with the supplier for clarifications.

[10] American Institute of CPAs (AICPA) https://www.aicpa.org/content/aicpa

[11] International Organization for Standardization (ISO) ISO/IEC 27001 https://www.iso.org/isoiec-27001-information-security.html and International Society of Automation (ISA) ISA/IEC 62443 https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

6. Solution Provider Security

In providing these services and benefits, solution providers become part of the entity's supply chain, and as such should be assessed for potential supply chain security risks.

The entity is encouraged to perform an assessment of the solution provider's security posture, possibly to a greater extent than they would evaluate any other supplier. While conducting the risk assessment of the solution provider may be challenging, it is critical because potential security risks or concerns present at the solution provider could be systemically introduced to the entity.

The NATF Model can guide an entity through the assessment process, and complimentary tools that guide an entity through specific actions such as conducting risk assessments[12] and incorporating procurement language,[13] plus others, can be of assistance. The NATF Model takes a risk-based approach and invites solution providers (as suppliers for entities) and entities to work together to determine mitigations to address identified risks. In the case of solution providers, there are unique considerations given the scope of the services. Here are areas to examine more closely:

- Which third-party certifications do they possess?
- Does the solution provider offer assurance of their processes?
- Do they house BCSI content?
- How is supplier proprietary data handled and protected?

Solution Provider Third-Party Certifications

It is important to know if the solution provider is certified to industry standards. This signals that there is accountability and adherence to best practices. Solution providers should provide the types of certifications they have received and how often they are evaluated. Some examples of relevant assessments/certifications are as follows:

- SOC 2 Type 2[14]
- ISO 27001[15]
- NIST SP 800-171/CMMC[16]

BCSI Considerations

Generally speaking, information about supplier practices and internal controls should not be considered BCSI. The details regarding the entity's security controls for their operations should not be exchanged between the

[12] American Public Power Association: Cyber Supply Chain Risk Management, https://www.publicpower.org/resource/cyber-supply-chain-risk-management
[13] Edison Electric Institute: Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf
[14] American Institute of CPAs (AICPA) https://www.aicpa.org/content/aicpa
[15] International Organization for Standardization (ISO) ISO/IEC 27001 https://www.iso.org/isoiec-27001-information-security.html
[16] Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/updates.html

entity and either the supplier or solution provider. However, when assessments of products or systems specific to the security of grid operations are performed, an entity should undertake efforts ensure that BCSI data is either not included or the solution provider and entity have devised secure practices for handling such information. Entities should avoid using IP addresses, hostnames, or security configurations of systems that will be used by solution providers to analyze supplier risks.

Supplier Proprietary Data

For many solution providers, proprietary information about the supplier's control environment or systems level controls is kept confidential between the solution provider and the supplier. For instance, a solution provider may submit a question to the supplier about their log management and automation processes. The details of systems and process may not be divulged to the requesting entity but the conclusory data (i.e., references to procedural documentation and summary findings) can be provided. This enables the entity to understand whether certain controls are being met, while allowing solution providers to effectively protect the details of practices that the supplier deems confidential. In addition, many solution providers provide a means of specific or sensitive information exchange between the entity and supplier for additional transparency of risk assessment activities.

7. Conclusion

There are multiple benefits solution providers can offer to entities in managing potential supply chain risks.

Solution providers can benefit entities by providing services that add value to an entity's supply chain security risk management efforts, regardless of the entity's available resources. Entities can research solution providers' offerings and determine the best fit for its organizations' needs. This guide provides information an entity should consider when selecting a solution provider. While not everything in this guide applies to every entity's decision, every entity should be mindful that a solution provider is another supplier to the organization, and as such entities should conduct a security risk assessment for any solution providers being considered. The NATF Model is an excellent roadmap for assessment of any potential solution provider and supplier. The NATF Model streamlines industry efforts to assess and manage supply chain security risks and is leveraged by solution providers in conducting supplier assessments.