Public Meeting on DHS Request for Information (RFI) “Cyber Supply Chain Risk Management”
RFI Number: RNCC-18-60068
Software and Supply Chain Assurance Forum, Fall 2018
Questions/Answers

Question: Is the next phase a Request for Proposal (RFP)?

Answer: Currently, this is limited to a Request for Information (RFI). It may serve as market research for an eventual RFP in FY2019, but that has not been determined and will be based on budget.

Question: What is your ultimate intent regarding sharing risk assessment information beyond DHS? Will the assessments be shared among government agencies, federal contractors, or is there a broader audience in mind?

Answer: Our intent is to share this information among all stakeholders, but before sharing any information, DHS will review any potential legal issues or implications. Any potential negative assessment of a company or product must be supported with objective evidence. The DHS National Protection and Program Directorate (NPPD) has been working closely with the DHS Office of General Counsel (OGC) to verify DHS’ authority to share supply chain related information amongst federal Departments and Agencies (D/As). However, it is unclear whether that authority extends to State, Local, Territorial or Tribal governments or the private sector.

Question: Are you looking for a services-based cloud? If so, do you expect to bring in FedRAMP software as a service (SaaS) or platform as a service?

Answer: We do not have a preference towards any specific type of solution. If you do happen to have a cloud-based solution, let us know whether it is FedRAMP authorized in your RFI response.

Question: Are there other federal D/As, for example the Department of Defense (DOD), which currently use a cyber supply chain risk management process that you are hoping to emulate?

Answer: Currently both the DOD and the intelligence community (IC) have cyber supply chain risk management capabilities. However, much of their work is classified. DHS is focusing this RFI on capabilities to collect and analyze open source data and is aiming to share the information it would collect more broadly. In addition, there are civilian agencies (non-DOD, non-IC) that have similar cyber supply chain risk management programs. The Commerce, Justice, and Science Appropriations Act has a requirement that certain agencies (e.g. Commerce, Justice, NASA, National Science Foundation) conduct supply chain risk assessments for all of their FIPS high and moderate IT purchases. DHS is engaged with these stakeholders and reached out to them for help when drafting the RFI.

Question: Will DHS inform this new solution about what the relevant cyber risks are? Or is the expectation that data will come into the solution about companies, people, products, services and capabilities and it will develop a set of risks that then need to be managed?

Answer: The answer is somewhere in between. Regardless of the direction of the information, our goal is to identify threats, weaknesses, and vulnerabilities in the ICT supply chain. Specific information might come from a DHS operations center or it could come from open sources; ultimately, we would want to use the cyber supply chain risk management solution to identify where these risks are in the cyber supply chain.

Question: Will this effort have plans for an unclassified as well as classified side to information sharing?

Answer: DHS is working closely with our IC partners. They will be involved in the process of analyzing the information. The information DHS collects will be made available to the IC, and DHS is exploring ways to infuse the collected open source information with intelligence. For example, if a group of companies is identified that is providing critical goods/services, DHS may share the list of companies with IC partners to get their opinion on which of those company/s DHS should focus its efforts on. IC would be able to indicate which companies would be worth keeping an eye on without having to divulge the classified explanation of why. Although it might not happen frequently, a case could arise where an open source analysis could show that a company's risk does not exceed risk tolerance in an unclassified environment but the IC may have information that would push it past the threshold in a classified environment. There is a high degree of correlation between what you can find in open sources in terms of derogatory information and what we find in classified sources.

Question: Do you prefer a solution to be a product delivered to DHS or information provided to DHS analysts or a combination of both?

Answer: Could be a combination of both, we need analytic capability and technology to help this process and aim for automation.

Question: Could you define what provenance is?

Answer: Provenance refers to the chain of custody during a product's development and delivery. In this case, it is part of threat traceability. It is mostly related to hardware, but provenance applies to software as well. Hypothetically, this traceability could go all the way back to the source.

Question: What are markings?

Answer: Markings of packaging.

Question: How will you avoid being overwhelmed by data?

Answer: That is the goal of RFI. There is no way to ingest all data feeds but the desired outcome is to improve awareness. DHS wants to be able to calibrate the risk assessment to the risk tolerance of the end user/company.

Question: Will you consider having one-on-one meetings with companies if they reply to RFI?

Answer: Yes, depending on volume of responses to RFI and quality of all those responses.

Statement: The level of information that potential vendors can supply in a RFI will be different than the level of information they can disclose in a one-on-one private meeting with the government.

Response: Many companies do supply chain risk management well internally but is not part of their service offering. Part of the motivation for the one-on-one meetings is to learn how they manage their internal ICT supply chain risk management.

Question: Has there been any discussion on whether this is more of a business intelligence function or an attempt to avoid that risk of possible intelligence oversight doing collection and analysis of U.S. businesses and entities?

Answer: There are important rules, statutes, regulations, and executive orders that control collection and use of information about US persons collected by the US IC. The goal is to avoid that.

Question: After reading the RFI, it seems likely that no one vendor will be able to respond to all parts. If you move forward in an RFP, will DHS frame it so that entities can apply to a piece of it, or will vendors be expected to develop a full solution?

Answer: Because the focus is still on the RFI, there is no definitive response. However, it is possible that there could be separate line items. RFI responses will help us determine which way to go.

Question: Have you considered implementing any type of enhanced category management initiatives to trim the supplier counts so that you cannot only have them register but validated, vetted, and hosted through a chain of custody?

Answer: On the topic of a reduction in the number of federal contractors, there are some implications for the Competition in Contracting Act and the basic procurement laws that underpin the federal acquisition system and any such goal would be outside the scope of DHS authority. The Continuous Diagnostics and Mitigation (CDM) approved products list is an example of what we see as a good outcome. DHS has a process in place with GSA where DHS added a line item to a GSA contract specifically for CDM tools, so if a vendor wants to sell their product to the CDM program, they must submit a package to DHS, including the functional requirements of the tool and a product assurance section.

Question: Is there an idea around the size of the ingested data? What are you going to want to manually monitor or have monitored on an automated basis?

Answer: That is beyond the scope of the RFI. There is a learning curve on the government side as to what we can do with this information. There is a two-fold problem: there are too many companies to assess and the government does not have capacity to consume that much data. Education and training will be a big component too.

Question: Can you talk about the end user community that will be exercising the solution? In particular the volume, type of user, the kind of experience you envision them having?

Answer: It runs the gamut. It includes the IT Security, CIO/CISO, Chief Security Officer, Chief Procurement Officer communities, and potentially others. It is another learning curve aspect, and it can vary organization to organization. Ultimately, it will potentially be a “follow the money” exercise down to the program level. People who are spending money on IT will have to be involved in using the information, independent of corporate organizational structure.

Question: It sounds like DHS has a Concept of Operations. If so, what might that look like? How will you ensure the validity of the information input into this database repository? For example, if someone does not care for an interaction with my company and puts something in that is not accurate. How do you vet, remove or wash the input data? Is there a decision yet on whether there will be a repository?

Answer: The intent is not to hoard information but to use it as the basis to engage in productive dialogue with companies. These decisions have not been made as to a repository or where it will be located, etc. This year, DHS is initiating some related work with some of its partner agencies. If this process unearths actionable information, DHS will share it. Shelf life and/or veracity of data will be considered. Shelf life: some data elements (e.g., name, address, physical location) will not change frequently, other elements will change often. For each risk indicator, we need to figure out what the appropriate shelf life is. Continuous data monitoring will also have an impact. Veracity: we want data from an authoritative source. There is a part of the RFI that addresses this.

Question: Will data feeds have to be “privacy sensitive” so companies are protected? And will companies be able to go in to see what is correct about them?

Answer: Yes, there will be privacy issues, and going forward that will be addressed. There must be a balance between having the information to make the assessment, and maintaining the information, which might put privacy at risk.

Statement: Given that most cyber assets are connect, enabled, and controlled by software, you may want to ask questions to better manage continuous nature of evolving landscape.

Response: An example of a supply chain risk mitigation DHS might recommend to a partner would be that every time you get a software update, you look at the bill of materials and see what is going into your software enterprise before you deploy it.