January 29, 2021

NCPS Program Management Office
Cybersecurity and Infrastructure Security Agency
tic@cisa.dhs.gov

Re: Internet Association's Comments on the Draft of Volume Two: Reporting Pattern Catalog of the National Cybersecurity and Protection System (NCPS) Cloud Interface Reference Architecture (CIRA) Documents (NCIRA)

Dear NCPS Program Management Office:

Internet Association (IA) represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our companies are global leaders in the drive to develop lower cost, more secure, scalable, resilient, and innovative cloud services to customers in both the private and public sectors. IA members include not only the leaders of commercial cloud-based solutions, but they also represent leaders within the Defense Industrial Base (DIB) and among the civilian contractor community at all levels from local to state to federal government.

With this experience in mind, IA and our members thank the NCPS Program Management Office (PMO) within the Cybersecurity and Infrastructure Security Agency (CISA) for continuing to engage with industry and the public in their efforts to implement standardized reporting patterns as part of the larger efforts to allow Government applications and services to take advantage of cloud computing and cloud-native features and functionality.

The Draft of Volume Two: Reporting Pattern Catalog (PDF) is a positive step towards ensuring the optimal use of the shared responsibility model among public sector programs, especially those who utilize more than one cloud service provider (CSP). In order to provide the best possible guidance to the users of this document, IA recommends that CISA incorporate the following feedback.

Provide For Continuous Comment Submissions On Reporting Patterns. IA applauds CISA for developing the standard format for each reporting pattern outlined in Section 1.3. This not only makes it easier to review existing reporting patterns, but to quickly create new ones. As the need for new reporting patterns indicates and the NCPS PMO staff undoubtedly are aware, technology is not static. As a result, updates and upgrades to the infrastructure that underpins much of the technology used by CSPs may require modifications to *existing* reporting patterns, including those provided for in this document itself.

Whether through the use of a public git-based repository (e.g., CISA's GitHub organization already has a repository focused on documentation associated with Binding Operational Directives (BODs) that can be used as an initial framework) or some other form of publicly available medium and collaborative forum, this will give CISA the ability to iterate on the reporting guidance in between official releases. The ability

to stay up-to-date as well as the opportunity for users within the federal government to easily provide feedback will give employees and contractors an avenue to contribute to something many already feel ownership over - the security of the networks they manage and operate.

Provide The Reasoning For CISA's Preferences Related To Cloud Telemetry Characteristics. IA is appreciative of CISA providing their preferences in relation to the reporting pattern-level characteristics related to cloud telemetry timeliness, timing coordination, and within the CISA Preference box in Sections 2.1, 2.2, and 2.3. While the CISA Preferences themselves are helpful, additional detail about the reasoning behind why those exact metrics were chosen would provide an additional level of insight necessary to help inform negotiations, especially in those instances where an agency or department may find it necessary to diverge from the CISA Preferences for any reason.

In Section 2.1 Cloud Telemetry Timeliness, CISA indicates the "goal is to detect, investigate, and respond to **any threat** before it has time to evolve and progress" (*emphasis added*). In order to achieve this goal, under the CISA Preference, when raw logs are not sent directly to CLAW by the CSP, CISA indicates that no more than 30 minutes should elapse between receipt of those logs by the agency and submission of those logs to CLAW after processing by the agency. It would help if CISA were to clarify the following:

- Whether this is a "preference" or a requirement, as the language right before the CISA Preferences box indicates that "[a]gencies **should ensure** that the time [...] is within 30 minutes" (*emphasis added*).
    - This would help clarify whether and how it would be possible to justify a time of delivery that exceeds 30 minutes.
- Why is a period of time of 30 minutes acceptable if the goal is to respond to "**any threat**" and Appendix A indicates that "Russian actors were found to have an average breakout time of under twenty minutes [which] is significantly faster than what many organizations are prepared to handle."
    - This would help in the development of a risk-based prioritization in those instances when agencies or departments may have to stagger their reporting or where an agency or department has assets of varying degrees of "attractiveness" and thus a necessity to apply varying cyber-relevant timeframes across their enterprise.
- What is the relevance of "log completeness", as mentioned in Appendix A, to this characteristic and what is the implication of an incomplete log, whether that lack of completeness is intentional or not?
    - This would help in providing a more complete understanding of the importance of this factor when negotiating this metric and providing an opportunity for agencies and departments to better understand the reasoning for the occasional lack of certain data and information, making their reporting more accurate and analysis more impactful.

In Section 2.2 Cloud Telemetry Timing Coordination, CISA outlines how important a standardized timestamp is to the performance of data analysis. As indicated in the language of this section, industry has widely adopted this principle. In order to achieve an accurate view of the landscape, the CISA Preference indicates that an agency should, "when feasible," preserve the "cloud-native telemetry timestamp". It would help if CISA were to clarify the following:

- When has an agency or department actually been in a situation where it was not feasible to preserve a cloud-native telemetry timestamp and what was done to account for it.
    - The rarity of these situations where it is preferable to use a different format would help to encourage and incentivize making it a requirement rather than just a preference or recommendation to adopt the usage of preserved cloud-native telemetry, especially in instances where a legacy system or process may otherwise be incentivizing otherwise.
- What is the easiest way to integrate the adoption of the cloud-native telemetry timestamps that CLAW is currently ingesting directly from CSPs in the development of new programs or projects.
    - This would provide a standardized way in which new infrastructure or applications that are integrated into a network manage and handle this data while widespread adoption of such best practices would also allow for an easier way to make wide-spread changes should they be necessary.

In Section 2.3 Cloud Telemetry Provenance, CISA provides several uses of provenance-related data, both in terms of providing the government with analytical capabilities and in providing visibility into potential causes of issues when performing troubleshooting. Appendix C provides even further detail, especially in terms of multi-tenant situations that may collect provenance data in different ways or at different times. In order to ensure those compiling the data can present it to those using it in a format that best suits their needs and those using the data can rely it on for critical activities, the CISA Preference indicates a requirement to convey provenance data "at sharing initiation and on an ongoing basis." It would help if CISA were to clarify the following:

- Whether this is a "preference" or a requirement, as the language in the guidance uses the word "must" when referencing the conveyance of the provenance of cloud telemetry.
    - This would remove any doubt about the requirement and associated timeframes of sharing provenance data.
- What is the easiest way to collect and convey cloud telemetry provenance-related data that CISA finds to be most useful and what information would be useful when an explanation of a change in such data is required.
    - As with Cloud Telemetry Timing Coordination, this guidance would provide a standardized way in which new infrastructure or applications that are integrated into a network manage and handle this data while widespread adoption of such best practices would also allow for an easier way to make wide-spread changes should they be necessary.

If possible, it would perhaps make more sense to change CISA Preferences to CISA Minimum, and establish a baseline that must be met. The language for at least two of the three cloud telemetry-related characteristics is written such that it is undeniably a requirement rather than a preference and making that clear would allow for more efficient negotiations on at least those points.

Share Statistics Related To The Usage Of Reporting Patterns At Least Annually. IA is supportive of the inclusion of Section 3.0 Generic Reporting Patterns and Section 4.0 Combination Reporting Patterns. While IA agrees with the conclusion that "it is not practical to discuss every possible permutation", there is great value in the ability to measure and identify patterns in terms of the usage of particular reporting patterns, including those not mentioned in this document.

Sharing this data will allow CISA, agencies and departments looking to make decisions related to patterns to use themselves, as well as industry to be both proactive and effectively reactive in circumstances where certain reporting patterns can be used to identify specific issues that need to be addressed. Whether through a publicly accessible medium, during regularly scheduled industry engagements, or any other preferred format, providing stakeholders the ability to use these usage statistics to make decisions will be invaluable, especially for those agencies or departments that end up having to use some of the least used reporting patterns and are looking to learn from the experiences of others.

In conclusion, sharing additional information in the form of CISA's reasoning behind their preferences, when those preferences are actually requirements, as well as statistics related to reporting patterns actively in use would benefit the users of this document.

As always, IA and our individual members are always appreciative of the time of NCPS PMO staff, CISA staff, and all cybersecurity professionals across the federal government invest in developing this type of guidance. We are always happy to make ourselves available to discuss any of our recommendations provided in this submission - or other topics of interest to you - in further detail.

Most Respectfully,

Omid Ghaffari-Tabrizi
Director, Cloud Policy