Confidentiality Coalition Principles on Cyber Incident Reporting

The Confidentiality Coalition strongly supports efforts to strengthen the nation's cyber defenses and to protect its critical infrastructure, including the healthcare industry, from cyber attacks. We also believe that enhanced information sharing and collaboration between the public and private sectors is essential to these efforts. Below are the principles that should inform any cyber incident reporting proposals.

1. **Reportable incidents should be well-defined and material.** Organizations should be provided clear, objective, and well-defined criteria for determining which incidents to report, and reporting should be limited to those incidents that are material and have the potential to cause harm to critical infrastructure. This is important not only to ensure consistency and provide meaningful data to the government, but also to ensure that reporting entities are not held to subjective, vague or overly broad reporting requirements. Organizations should not be required to report "potential" or "suspected" incidents or minor incidents that do not have the potential to affect critical infrastructure.

2. **The time frame for reporting should be without unreasonable delay but no sooner than 72 hours after an incident is confirmed.** Time is of the essence in containing a cyber incident, and organizations should be allowed a minimum of 72 hours after a breach is confirmed to focus first on addressing the incident, and then to determine whether reporting is required and, if so, to gather and report the required information to the government. Requiring reporting any sooner will compel organizations to focus on their reporting responsibilities rather than on addressing the incident itself. In addition, because organizations will not have sufficient time to gather the information necessary to assess whether an incident is reportable, an overly short time frame will cause organizations to overreport, making reports less useful to the government. This is particularly the case if reporting is required for "potential" incidents, and so before an organization has had the opportunity to confirm that an incident has occurred. The time frame for reporting should begin only once an actual incident has been confirmed.

3. **Only entities that suffer the cyber incident should be required to report it.** While affected entities should be permitted to delegate their reporting responsibilities to service providers or others, only the affected entity should have a responsibility to report an incident. No entity should be required to report an incident that occurs at another entity, whatever the relationship between the two entities. Such a requirement would engender distrust between entities, causing them to be less willing to share information or utilize outside experts, and is more likely to result in inaccurate or incomplete information.

4. **Reporting entities should be of a minimum size, appropriately defined.** Health care organizations and other operators of critical infrastructure recognize the importance of their services to public health and safety, and therefore, the importance of government

awareness when the industry suffers cyber attacks. However, since many cyber incidents are indiscriminate and the affected entity may be small or inconsequential from a public health or safety perspective, reporting should be limited to only those entities where there could be a material impact on critical infrastructure.

5. **Avoid multiple reporting requirements for a single incident.** Many entities that will be subject to cyber incident reporting are already subject to various federal and state reporting requirements. Healthcare entities in particular are subject to HIPAA breach reporting requirements and state data breach reporting requirements, to mention only two. Any cyber incident reporting proposals should take into account existing reporting obligations and endeavor to avoid duplicative, multiple or inconsistent reporting. Harmonizing reporting requirements so that each entity is required to report a specific incident only once and to a single government agency will streamline the reporting process, avoid double counting, and allow both affected entities and government agencies to utilize their resources more efficiently.

6. **Provide for a meaningful, but not punitive, enforcement mechanism.** To be effective, any reporting mandate must have a meaningful enforcement mechanism. However, a structure based on providing incentives to report, such as liability protections -- and the loss of those incentives for those who do not report as required -- is more likely to result in compliance and collaboration than one based on the imposition of civil or criminal penalties. This is particularly the case for organizations that have been the victim of a cyber attack, where government action should be supportive, rather than punitive, to engender mutual trust and cooperation to build national resilience.

7. **Organizations should be provided comprehensive liability protection for reporting.** Reporting entities should have the assurance that they will not face legal liability as a result of providing a cyber incident report. This assurance should include protection from civil and criminal liability, as well as from regulatory enforcement of any kind based on the fact of reporting or the contents of any report. This is important not only as a matter of fairness, but also to ensure the quality and integrity of the reporting, and so that reporting entities can focus exclusively on providing the most detailed and comprehensive information available, rather than protecting themselves from potential liability. Without the assurance of liability protection, organizations will be reluctant to report as openly, and may limit or color the information provided, while still meeting the minimum requirements.

8. **Limit information requested and used to the purpose for which reporting is required, including to disseminate cyber alerts and guidance to industry.** In addition to liability protections, reporting organizations should be assured that the cyber incident information required to be reported is strictly limited to that which is needed to identify and respond to cyber incidents effectively, and to disseminate cyber alerts and related information to industry participants to help them guard against or mitigate similar attacks. Reported information should be treated as the confidential and proprietary information of the reporting organization and disseminated only in anonymized form that protects the reporting entity's identity. The information should be exempt from state and federal freedom of information disclosure laws and regulatory use beyond the goals of the cyber incident reporting law itself. This will result in reporting entities sharing information more freely with the government and allow for more open and useful information sharing towards the common goal of cyber attack prevention and deterrence.

9. **Require full rulemaking process to allow meaningful opportunity for stakeholder input on any cyber reporting regulations.** Since some of the most significant aspects of the cyber reporting requirements will be specified in regulation, it is imperative that the Cybersecurity and Infrastructure Security Agency (CISA) or any other relevant government agency allow for robust stakeholder input before promulgating a regulation. This should include, at a minimum, a proposed regulation with a 90-day comment period. This will provide the government with critical information needed to shape a regulation that is targeted, clear and realistic, which will in turn result in greater compliance and more useful information for the government.