NCI Principles on Mandatory Reporting

The National Council of ISACs has been facilitating cross sector information sharing since 2003. The NCI and our members are committed to continuing to improve sharing across the NCI Membership, within the individual members, and between industry and government. As policy makers consider implementing mandatory reporting requirements, the NCI believes that it is important policy makers consider the following:

Scoping

- Who does the proposal apply to? The more narrowly focused the better since there is a limit to how much information CISA, or any organization, can intake, process and analyze.
- What needs to be reported? Enterprises must understand what incidents they are required to report.
- When do they need to report it? Enterprises need to know when the clock starts ticking for reporting requirements.
- Where does the information need to be reported? Some industries already face mandatory reporting. Requirements should be harmonized so that organizations are not reporting the same information multiple times to different agencies.

Cost and Benefit

- Implementing mandatory likely will divert limited resources from security to compliance. Government needs to fill this gap by providing timely and actionable intelligence and analysis to critical infrastructures.
- Government should articulate how mandatory reporting will improve security. There is no benefit to incident reports sitting in a database. To return value to industry, CISA should provide Substantive warnings and lessons learned from what has been reported.
- Codifying "tear line" information with ISACs for distribution to their members would be another way CISA can add value and rapidly disseminate information to thousands of critical infrastructure owners and operators. Sharing sensitive but unclassified information about sectors incidents and those against related interdependent sectors will prompt action by owners and operators. Sharing this information through ISACs allows sector experts to add context and best practices to the reports. Without enactment of legislation to require such sharing from government, history clearly shows that little such sharing will occur.
- Turning CISA into a regulator/semi-regulator will impact their partner relationship with the critical infrastructure community. Will the benefit of the mandatory reporting and compliance, and the potential of fines, outweigh this cost?

Blame the Malicious Actors, not the Victims

- Critical infrastructure owners and operator should take appropriate steps to secure their networks, but it is counterproductive to blame victims, especially those that are victims despite implementing appropriate security protocols.
- There is no cost to the adversary. There are no consequences on nation-states for their activities, and most cyber criminals are able to avoid action by law enforcement. Until we start imposing consequences for this behavior on malicious actors, they will continue to attempt to disrupted critical infrastructure.

Leverage Existing ISACs to ease Implementation

- Mandatory reporting should not replace or serve as a disincentive to voluntary engagement in information sharing organizations. Public policy should recognize the trusted role ISACs play in their sectors and codify collaboration among ISACs, CISA and Sector Risk Management Agencies.
- ISACs can be a natural conduit to make it easier for critical infrastructure to comply/report. Use ISAC infrastructure to enable simultaneous reporting and to disseminate intelligence from DHS to industry. Requiring DHS to engage with ISACs in this manner will help grow these trusted communities and provides much needed scaling to DHS' efforts.
- The same liability protections should apply to the same information whether it is shared with industry or government. If there is greater liability protection for information shared with government than industry, there is an incentive for companies to not share with partners through ISACs.