# Executive Order 13636 – Improving Critical Infrastructure Cybersecurity<br>Section 10(b) Report on the Department of Homeland Security's<br>Chemical Facility Anti-Terrorism Standards

## Background

On February 12, 2013, the President issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity. Under Section 7(a) of EO 13636, the National Institute of Standards and Technology (NIST) was directed to develop a Cybersecurity Framework (Framework) to reduce cyber risks to critical infrastructure. Pursuant to Section 10(a) of the EO, all agencies with responsibility for regulating the security of critical infrastructure are required to review the preliminary Framework and determine if current cybersecurity regulatory requirements are sufficient in light of current and projected risks.

Within the Department of Homeland Security's National Protection and Programs Directorate (NPPD), the Infrastructure Security and Compliance Division (ISCD) has regulatory authority over security at high-risk chemical facilities pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27. To meet the requirements of EO 13636 Section 10(a), ISCD assessed the cybersecurity standards implemented under CFATS to determine if they are sufficient given current and projected risks associated with chemical industry infrastructure. To accomplish this, ISCD and the Office of Cybersecurity and Communications (CS&C) compared the metrics developed for CFATS Risk Based Performance Standard 8 (RBPS-8) on cybersecurity with the NIST Framework to determine if any significant gaps existed. On February 10, 2014, NPPD provided a Section 10(a) report to the White House detailing the results of that analysis.

Based on the analysis, NPPD determined that there were no significant gaps between CFATS RBPS-8 and the NIST Framework, and that CFATS was addressing cybersecurity in a sufficient manner. Specifically, the analysis determined CFATS RBPS-8 had metrics that were equivalent to 53 of the 97 subcategories contained in the NIST Framework, and metrics addressing an additional 21 of the 97 subcategories contained in the NIST Framework, but at a different level of granularity than the NIST Framework. For instance, CFATS Metric 8.4.1 broadly addresses the need for facility employees to receive role-based cyber security training, while the NIST Awareness and Training category has five subcategories detailing specifically who should receive training (e.g., general users, third-party stakeholders, senior executives). The overlap between CFATS and the NIST Framework for these 21 subcategories was assessed to be sufficient enough to not consider these a significant gap between the two programs.

The CFATS guidance for RBPS-8 does not have equivalent metrics for 23 subcategories contained in the NIST Framework, which can be grouped in the following areas:

- Identification/declaration of various items, such as the organization's role within the industry, mission and objectives, and risk tolerance level *(8 subcategories)*
- Securing sensitive business information through, for instance, the protection of intellectual property and personally identifiable information (PII) *(5 subcategories)*
- Coordinating and communicating with stakeholders, to include managing public relations and engaging in post-event reputation rehabilitation *(4 subcategories)*
- Risk assessment activities related to threats and potential impacts *(3 subcategories)*
- Miscellaneous policy requirements, such as ensuring adequate storage capacity and implementing configuration change controls *(3 subcategories)*

Despite the lack of an equivalent CFATS metric for these 23 items, NPPD concluded that there is no significant security gap between the two regimes. The majority of the unaddressed subcategories, such as identifying the organization's role within industry and managing public relations, are best practices that are not necessary for the prevention of a terrorist attack on a chemical facility; or, in the case of the risk assessment activities, already are being conducted by NPPD and the facility through other portions of the CFATS program, and thus are properly not included in the CFATS RBPS metrics. A small number, such as protecting removable media and requiring configuration change controls, were determined to have the potential to strengthen the cybersecurity requirements under CFATS and may warrant future consideration for inclusion; however, none were identified as significant gaps warranting immediate corrective action.

**Path Forward**

Under EO 13636 §10(b), "if current regulatory requirements are deemed to be insufficient . . . agencies [that were required to complete a §10(a) report] shall propose prioritized, risk-based, efficient, and coordinated actions . . . to mitigate cyber risk." As noted above, NPPD's analysis of the CFATS requirements under §10(a) resulted in a determination that the CFATS cybersecurity requirements are sufficient, and there are no significant gaps between the CFATS requirements and the NIST Framework. Nevertheless, ISCD is planning actions to address the minor differences between CFATS cybersecurity requirements and the NIST Framework, and, at the White House's request, ISCD has developed this §10(b) report to provide a summary of those planned actions.

To address the minor differences that currently exist between the CFATS RBPS-8 on cybersecurity and the NIST Framework, ISCD intends to undertake two activities:

(1) For those items within the NIST Framework that directly address cybersecurity (e.g., protecting removable media; requiring configuration change controls) and that are not currently addressed within CFATS RBPS-8, ISCD will explore making modifications to the CFATS RBPS Guidance Document so that CFATS-regulated facilities consider measures to address those items when developing their site security plans. ISCD intends to commence efforts within the next couple of years to update the CFATS RBPS Guidance Document in conjunction with rulemaking efforts to update the CFATS regulations themselves, and updates to the cybersecurity portions of that guidance document would be done as part of this overall effort.

(2) As noted above, the remainder of the differences between the NIST Framework and CFATS RBPS-8, are either best practices that are not necessary for the prevention of a terrorist attack on a chemical facility (e.g., identifying the organization's role within industry; managing public relations) or, in the case of the risk assessment activities, already are being conducted by ISCD and the facility through other portions of the CFATS program, and thus are properly not included in the CFATS RBPS metrics. These activities do have value as part of an overall approach to risk management, however, and in recognition of that value, NPPD will develop and publish a fact sheet or other document encouraging high-risk chemical facilities to consider the voluntary adoption of these other items from the NIST Framework.

Consistent with EO 13636 §10(c), in two years, the Department will provide a report to the White House's Office of Management and Budget on the progress made in implementing the two actions described above.