Appendix - Language for Consideration

By Nicholas Leiserson

As a starting point for policymakers, this appendix provides sample language that may prove useful in applying the approaches laid out in the ***Last Mile Cybersecurity Policy Memo***.

Agency-Specific Approaches

For Congress

Lawmakers can build upon language included in the Bipartisan Infrastructure Law for specific grant programs.

"Sec. Cybersecurity Plans and Risk Mitigations

a. In General.---The Secretary shall require a recipient of any award or other funding under this program—

1. to submit to the Secretary, prior to the issuance of the award or other funding, a cybersecurity plan that demonstrates the cybersecurity maturity of the recipient;
2. for projects that contain and use programmable electronic devices essential to the reliable operation of critical infrastructure, to submit to the Secretary, prior to the issuance of the award or other funding, a project cyber risk assessment and a project cybersecurity plan.

b. Project Cyber Risk Assessments.---A project cyber risk assessment described in (a) shall, at minimum, detail:

1. Threat modeling used in conducting the assessment.
2. A list of common cybersecurity controls, such as the Cybersecurity and Infrastructure Security Agency's Cross-Sector Performance Goals, and their applicability to the project.

c. Project Cybersecurity Plans.---A project cybersecurity plan described in (a) shall, at minimum, contain:

1. Identifying grant award information.
2. A high-level description of the plan for the overall management of the project's cybersecurity program, including a high-level description of how resources, roles, and responsibilities will be managed.
3. An inventory of project IT/OT technology assets.
4. A list of planned cybersecurity risk mitigation actions and controls, including:
   A. A prioritized list of assessment gaps that need to be addressed; and
   B. A list of cybersecurity risk mitigation actions to be undertaken as part of execution of the grant award, with a target implementation date identified for each mitigation.

d. Annual Updates.---The project cyber risk assessments and project cybersecurity plans described in (b) and (c) shall be updated annually.

e. Auditing.---The Secretary shall provide guidance to appropriate offices within the Department to review project cyber risk assessments and project cybersecurity plans, in coordination with relevant technical agencies, as appropriate.

For the Administration

The ONCD Playbook has notice of funding opportunity (NOFO) and terms and conditions language that can be used by funding agencies. While the ONCD Playbook confined itself to critical infrastructure operations, the language could be generalized as well. The NOFO language is reproduced here for ease of reference.

"Project Cyber Risk Assessment and Project Cybersecurity Plan. Entities receiving funds through this program must ensure that cybersecurity is integrated into the design, development, operation, and maintenance of critical infrastructure information technology (IT) and operational technology (OT). Projects that contain and use programmable electronic devices essential to the reliable operation of critical infrastructure must complete certain requirements after receiving a grant award. These requirements include a Project Cyber Risk Assessment and a Project Cybersecurity Plan."

A Broad Baseline

A broad-based approach could be implemented by updating the Uniform Guidance. For instance, 2 CFR 200.211 could be amended (in bold below) to add a new general term and condition.

"(c) General terms and conditions.

1. Federal agencies must incorporate the following general terms and conditions either in the Federal award or by reference, as applicable:
    i. **Administrative requirements.** Administrative requirements implemented by the Federal agency as specified in this part.
    ii. **National policy requirements.** These include statutory, executive order, other Presidential directive, or regulatory requirements that apply by specific reference and are not program-specific. See § 200.300 Statutory and national policy requirements.
    iii. **Recipient integrity and performance matters.** When the total Federal share of the Federal award may include more than $500,000 over the period of performance, the Federal agency must include the terms and conditions available in Appendix XII. See also § 200.113.
    iv. **Future budget periods.** When it is anticipated that the period of performance will include multiple budget periods, the Federal agency must indicate that subsequent budget periods are subject to the availability of funds, program authority, satisfactory performance, and compliance with the terms and conditions of the Federal award.
    v. **Termination provisions.** Federal agencies must inform recipients of the termination provisions in § 200.340, including the applicable termination provisions in the Federal agency's regulations or terms and conditions of the Federal award.
    vi. **Critical cybersecurity controls. When it is anticipated that a recipient of an award with a total Federal share of more than $5,000,000 will contain and use programmable electronic devices essential to the reliable operation of critical infrastructure, the Federal agency must include the terms and conditions available in Appendix XIII."**

Sample terms and conditions can be found in the ONCD Playbook and would be appropriate to add as a new appendix to the Uniform Guidance.

Create a Cyber Set-Aside

Lawmakers considering allocating funding for projects on a fixed basis could consider adding language to particular program authorizations or appropriations.

Authorizations

In program authorizations, language could be tied to specific projects.

"Sec. Cybersecurity Funding Required—Of the funding used by awardees for information and communications technology and services, not less than 10 percent shall be used for a cybersecurity purpose, as that term is defined in Section 2200 of the Homeland Security Act of 2002 (6 USC 650)."

Appropriations

Appropriators, in contrast, might instead focus at the program level using historical data for ICTS spending. For instance, if 15 percent of award dollars for a particular program went to ICTS over the past several years, the go-forward set-aside would be 1.5 percent.

"$XXX,XXX,XXX for Program ABC, provided that $[10 percent of the funds previously used for ICTS] are used for a cybersecurity purpose as defined in Section 2200 of the Homeland Security Act of 2002 (6 USC 650)."