CSC 2.0

Thirteen Guidelines for Rewriting PPD-21

Mary Brooks, Annie Fixler & RADM (Ret.) Mark Montgomery

While there are outstanding questions on the intent, scope, and timeline of the Biden administration's policy review process for updating PPD-21, the following guidelines should shape any revision process:

1. **Clearly identify any change in strategic direction.** Without a change in strategic focus, a PPD-21 rewrite risks simply reshuffling the deck chairs. The geopolitical and cybersecurity environment has changed substantially, and PPD-21 must change accordingly. Clearly state the need for a better balance of regulation, incentivization, and collaboration to achieve a more resilient infrastructure. Also identify the new critical infrastructures that have emerged over the past decade — to include space systems and cloud computing industry.
2. **Make updates to processes with surgical precision.** The vision and strategy laid out in PPD-21, at 10 years out, is ripe for a change. Yet it also underpins decades of collaboration, relationship-building, and process. A whole-scale change — like removing the sector-by-sector focus — risks undercutting this work and leaving the country even more vulnerable in a crisis.
3. **Don't use policy as a catch-all for implementation problems — but ensure operational and implementation documents are updated.** Many of the weaknesses of the current national critical infrastructure protection framework are ones of implementation. They will not be resolved immediately with a policy rewrite and may even worsen in the short term.
4. **Create a mechanism to keep PPD-21 and supplemental policy documents updated.** Critical infrastructure protection documents should probably be updated biennially and certainly more often than once a decade.
5. **Define expectations for CISA as the NRMA.** CISA's success underpins the success of the national critical infrastructure protection framework. Its roles and responsibilities as the national risk manager should be made clearer, and it should be given the authority to realize them. And then it should be held accountable if it does not perform its role.
6. **Selectively strengthen CISA as the NRMA**. CISA has been given a tremendous amount of responsibility in recent years, and there is a hunger for it to do more — particularly in information sharing, risk analysis and management, and emergency response. This will require careful matching of resources to capabilities to tasking.
7. **Clarify SRMA roles and responsibilities.** Resolve any discrepancies between executive branch policy and FY 2021 NDAA language. Further provide clarity to ensure these issues do not resurface. But also recognize that not all SRMAs — and not all sectors — are the same and that flexibility is a must.
8. **Direct adequate resourcing of SRMAs**. Ensure agency needs as an SRMA are anticipated and included in the president's annual budget to Congress. Ensure Congress understands that funding domestic critical infrastructure protection is as important as buying F-35s.
9. **Solve the perennial question of who in the government to call during a crisis.** A company dealing with an emergency incident cannot be expected to call the FBI, CISA, and its SRMA. Make it easy to do the right thing.
10. **Revamp information sharing between the government and private sector.** A famously difficult task, this will require creating simple pathways that avoid over-classification of government information, resolving issues of liability and recognizing that private sector information is often better than government information, particularly on domestic issues. If this process is not simple to access, less-resourced companies and utilities may not be able to act on warnings.
11. **Establish a prioritization framework.** The government cannot simultaneously assist all infrastructure owners and operators equally. Establish a system to identify systemically important entities and work with Congress to develop a system of benefits and burdens.
12. **Create minimum physical security and cybersecurity standards hand in hand with industry.** Industry often knows what it needs, and minimum standards cannot be dropped from on high. Nonetheless, a completely voluntary model has repeatedly proven unsuccessful. There needs to be a new middle ground that achieves sufficient standards through a balance of regulation, incentivization, and collaboration.
13. **Require continuous communication with stakeholders.** Updating stakeholders in government and beyond in an iterative process. This is not the type of policy that can be held until a final version is decided upon.