Situation: Confirmed Interference in Presidential Election

Bottom Line Up Front (BLUF): We prioritize the following actions: (1) reform the validity of our election systems to ease public tensions, (2) induce the threat actor to cease interfering with democratic processes, and (3) fix endemic critical infrastructure flaws.

Context: Government sources have confirmed that an unidentified threat actor (TA) exploited a critical vulnerability in the energy infrastructure to cause power outages that prevented the collection of ballots in several states. We assess with high confidence that the TA did so to disrupt the 2020 presidential election. Despite election irregularities, the news sources have confirmed the election results, resulting in widespread discontent. Some resultant demonstrations have become violent, with unconfirmed casualties.

Unknowns:

- Legal standing for redoing elections
- Specific attribution of cyberattacks
- Strategic intent of threat actor

Threats:

- Potential for misattribution
- TA uses social engineering to exacerbate tensions and violence

Opportunities:

- Motivation to remediate persistent issues in election systems and cross-sector vulnerability

Mobilize a Cyber Unified Coordination Group (UCG)

- DHS mobilizes the ICS-CERT to work with local authorities to conduct penetration testing of networks
- FBI directs the NCIJTF to collect forensic evidence on cyber-attacks to validate attribution questions
- ODNI directs intel community to provide relevant information to federal agencies for release to state, local, private entities

Three Priorities: Secure Elections; Attribution; Critical Infrastructure

In order to ensure the long-term security of our elections, we must investigate the past election and reform our elections infrastructure, procedures, as well as partnerships to make them resistant to interference.

- President appoints nonpartisan czar to explain the immediate responses of our government and outline the facts of the election
- Utilize the Election Assistance Commission to reform current election infrastructure by increasing vote accountability and developing cohesive contingency procedures that polling stations should use in case of difficulties
- Increase the quality of private-public partnerships, especially with social media and communication companies, to prevent foreign actors from intervening in the election process and worsening tensions

Through the employment of diplomatic, informational, military, and economic instruments of power, we can determine attribution for these attacks and then prepare deterrence measures.

- Developing proposals of global standardization, binding norms, and rules as part of international law to address election interference and attacks on industrial control systems
- NSA will lead intelligence acquisition operations and work alongside intel sharing partners like Five Eyes
- Coordinated defensive operations between the USCYBERCOM and NSA to preempt escalatory actions
- Implementing or raising economic sanctions through bilateral partnerships with global trade partners serves as a punitive measure for meddling in American election systems, institutions, and infrastructure

Given cross-sector interdependencies, we must institutionalize and resource a process to identify them and ensure secure, functioning, and resilient critical infrastructure.

- Provide increased funding for the Sector Coordinating Councils to help critical infrastructure owners and operators outline a wide range of sector specific strategies, policies, and activities
- DHS development of a flexible emergency communications system that the public and private sectors can utilize
- Identify cross-sector independencies through TTXs to mitigate cascading failures and promote contingencies