## Team Blackjacks of the United States Military Academy

### Situation

Several power outages across numerous municipalities have begun to disrupt the ongoing 2020 presidential election. Members of the public, wary from the 2016 Russian election interference, believe the power outages are another attempt by a malicious actor to interrupt democratic processes. There is circumstantial evidence to support that hypothesis. For example, an industrial control system (ICS) developer has informed DHS that have discovered a critical vulnerability in a product widely-used in the energy sector. Additionally, reports indicate that Russian proxies (i.e. Sobornost) are recruiting former US intelligence operatives with experience in ICS exploitation. The government now faces the challenge of restoring public confidence in its democratic processes despite circumstantial evidence of ongoing foreign interference.

### Opportunities

- Restore public trust in elections and gov't effectiveness
- Foster coordination between Federal and SLTT entities
- Increase accountability amongst infrastructure operators
- Clarify roles and responsibilities for gov't and private sector
- Deepen ongoing intelligence sharing efforts like Pathfinder

### Threats

- Potential for ongoing interference or escalatory intentions
- Classified information and TTPs used by former intel operatives falling into the hands of foreign governments
- Premature action against an adversary without an evidentiary basis for doing so

## PPD-41

### Declaring a "significant cyber incident"

- DHS mobilizes the ICS-CERT to work with local authorities to restore power to affected municipalities
- FBI investigates the possibility of deliberate interference in the power grid with the NCIJTF
- ODNI directs NSA to provide relevant information to federal agencies for release to state, local, private entities

+

### Augmenting the Cyber UCG

- Recommend the Council of Governors convene to coordinate sharing of resources and expertise
- NSA executes FISA warrant to determine if former intel operatives disclosed classified information and methods
- DHS coordinates with DOE and E-ISAC to prioritize assets most critical to public safety

## Additional Policy Actions

### Election Systems Infrastructure

- President directs the EAC to aid municipalities in helping voters switch polling stations and voting with provisional ballots
- President holds a bipartisan press conference with Republican and Democratic leaders to reassure validity of elections
- President issues a strong statement reaffirming commitment to deterring foreign election interference

**Pros:** Bipartisan approach will not skew perception of action; allows election to proceed as best as possible under circumstances
**Cons:** Political leaders may not want to meet; statement may be escalatory

### Energy Infrastructure

- Prioritize the development of a flexible emergency communications system that the public and private sectors can utilize;
- Increase regulatory oversight of bulk-energy systems by the NERC to include mandatory analog backup systems
- Design a portfolio of incentives to include the private sector in the development of cross-sector analysis and resiliency.

**Pros:** Resiliency measures like analog systems will help in cascading events; gov't already working in emergency communication
**Cons:** Costly in terms of the time, training of personnel, and resources necessary for the development and implementation

### Broader Issues with Critical Infrastructure/Lifeline Sectors

- Provide reoccurring visits from ICS-CERT teams to validate systems at the request of private infrastructure operators
- Enforce accountability of ICS vendors to fix faulty software by mandating trust funds for creating patches
- Institutionalize regular table top exercises to preempt cascading effects and clarify roles and responsibilities

**Pros:** Promotes a culture of accountability in ICS development
**Cons:** ICS developers may respond to regulation with increased prices; CERT rotations and TTXs are resource intensive