Technical Questions (Page 1 of 9)

1. In the event of an incident, would we be expected to staff or respond to it?
2. In the event of an incident, who would our stakeholders be expected to call first?
3. How would we handle the meetings and operations of the Sector and Government Coordinating Committees?
4. What would the role of Testing and Certification be in the new environment, given its relevance to cyber security?
5. Given that EAC has a small regulatory role, how is the wall between that function and the protection of Protected Critical Infrastructure Information, or PCII, to be managed?
6. Would EAC need to designate staff or section to handle the physical security side, given we already have a section that handles cyber security?
7. In the event of a jurisdictional conflict over who should handle an issue, such as a public school system that views security of polling held on its sites as solely a school system or Education Sub-Sector issue, are EAC or DHS able to intervene?
8. What guidance can stakeholders expect regarding what risk and threat assessments to use?
9. Can EAC and DHS point stakeholders toward suitable training?

Technical Questions (Page 2 of 9)

1. Can EAC help stakeholders develop partnerships with entities that are eligible for grants that the stakeholders themselves cannot get?
2. Will training and grants specific to the election space be developed?
3. What role will stakeholders have with EAC in developing goals and milestones for CI security?
4. Would any CI discretionary grants be administered for the Sub-sector by EAC?
5. If yes, would the process be substantially different from the usual grant process?
6. Would any paperwork and reporting burden and process for CI discretionary grants administered by EAC be different from the current grants it administers?
7. Would any CI grants administered through EAC be handled by the same office?
8. Is the distinction between cyber and physical security seen in the DHS documents going to create issues during the actual conduct of an election?
9. To what extent would Testing and Certification be using information protected by the PCII exemption from FOIA, regulation and lawsuits?

Technical Questions (Page 3 of 9)

1. How will all stakeholders receive information about threats to their elections systems (voting systems, VRDBs, EPBs, polling places, etc.)?
2. Will EAC T&C receive information about potential threats or risks to systems currently certified or in the process of attaining certification?
3. What impact will this have on our VVSG?
4. What impact does this have on EAC accredited VSTL?
   A. What additional testing, experience, training will they need to have/conduct?
   B. What information will be shared with them, so that issues or concerns can be addressed during test campaigns?
5. Who will receive information about threats or attacks on election systems?
6. What information can be made public about the handling of threats or attacks?
7. How can stakeholders maintain transparency in the election administration process without violating rules imposed based on critical infrastructure determination?
8. Is there information shared by election officials currently that they will no longer be able to publicly share?

Technical Questions (Page 4 of 9)

1. How does this designation impact pilot projects for various types of election systems or processes?
2. Who is responsible for offering guidance related to CI on best practices for blank ballot delivery and electronic ballot return process, which is currently outside of the EAC T&C program?
3. Who will develop best practices/guidance related to securing VRDBs and EPBs?
4. Have all stakeholders been identified and is there a plan in place for what information will be communicated to each of those stakeholders? For example, stakeholders = election officials at state, local and federal level (including those with responsibilities/duties to update/implement/use VRDB, election day processes/prep, testing & certification, etc.), election system manufacturers, test laboratories or examiners, USPS, ballot printers, those hosting polling places, etc.
5. How will physical security requirements related to CI impact election offices, polling places, election system equipment storage facilities, election system equipment manufacturing and business facilities, voting system test laboratory facilities, etc.?

Technical Questions (Page 5 of 9)

1. Can a state volunteer to implement the suggestions/requirements without Federal assistance?
2. Would the States that apply for grants have to volunteer for the Federal CI assistance?
3. To what portions of the election process will CI apply?
4. How does the CI designation impact the auditing and validation of results?
5. Will vendors and other partners be defined, designated and/or recommended by DHS?
6. Will vendors be held to the same standards as election jurisdictions?
7. Who determines the stakeholders?

Technical Questions (Page 6 of 9)

1. Who falls within the designation of election officials: State agencies/employees, County agencies/employees, Municipality agencies/employees, Other elected local agencies/employees, and Precinct workers?
2. What is entailed in physical security: Physical security of the voting equipment, Physical security of the ballots, Physical security of ballot transportation, Physical security of the voting locations, and Physical security of the election offices?
3. In order to secure the location and equipment, will there be requirements restricting access to processes that are currently required to be transparent/open to the public, such as Logic and Accuracy Testing, Opening ballots, Sorting ballots, Ballot tabulation, Ballot duplication, Audits, and Recounts?

Technical Questions (Page 7 of 9)

1. Who is a vendor?
    - Ballot printer
    - Sample ballot vendors
    - Ballot pamphlet providers
    - Election mailer providers
        - Parties
        - NGOs
    - Voting System Manufacturer
        - COTS providers; and
        - EAC Registered Manufactures
    - Electronic ballot delivery systems
        - Military and overseas voters
        - Voters with disabilities
        - Email providers
        - Fax machine companies
        - Home computers, printers, & scanners
    - Voter Registration Database manufacturers
    - Polling Place lookup systems
    - Electronic poll book manufacturers, continued

Technical Questions (Page 8 of 9)

- Election night reporting manufacturers
- Ballot duplication system companies
- Adjudication/ballot reconciliation companies
- Archival companies
- Data backup locations
- Ballot delivery companies
  - USPS
  - UPS
  - FedEx
  - Other drayage companies
- Candidate filing system manufacturers
- GIS software providers
- Polling place providers
  - Churches
  - Schools
  - Private residences
  - Private businesses, continued

Technical Questions (Page 9 of 9)

Other governmental agencies that provide checks and balances against registration?

- SSA
- Courts
- Department/Bureau Motor Vehicles
- Local agencies maintaining birth/death records (County Clerk/Recorder)