From: Mitchell, Jeffrey R
To: [redacted]
Cc: [redacted]
Subject: RE: Witness Invitation Letter - Cybersecurity of Voting Machines 11-1
Date: Tuesday, November 28, 2017 4:47:00 PM

[redacted]

Thank you for your patience. As I discussed with you, NPPD made telephonic notifications. Below, I've excerpted the model script for the calls NPPD made last September to States believed to be targeted by Russian government cyber actors. These calls were made by several different people, and the basic script was utilized to ensure consistency in communications. As applicable, State-specific information was appended for use by the caller and follow-up contact information was provided.

I hope that this assists, but am happy to answer any additional questions.

Jeff

- Hello, this is [name] with the Department of Homeland Security's National Protection and Programs Directorate.
- I am calling today as part of my outreach to state election officials on the question of possible Russian cyber targeting of elections systems in your state and others during the run up to the 2016 presidential elections.
    - It appears that Internet-facing election infrastructure in your state was targeted by Russian government cyber actors.
    - They scanned your Internet-connected election infrastructure, likely seeking specific vulnerabilities, such as access to voter registration databases.
    - However, we are not aware of any attempts to exploit those vulnerabilities or other Russian activity directed at your election infrastructure.
- The owner or operator of the system in your state was notified at the time that we learned of this attempt. In your state, these were [appropriate office or entity].
    - Our policy is to maintain the integrity and confidentiality of the victims of cyberattacks. However, we realize that as the chief state election official you also have a need to know if your state was targeted.
    - If you have not already done so, I encourage you to reach out to the state contacts I mentioned if you would like to learn more about this incident.
    - Going forward, we are working on a way to alert you to incidents in your state, while still maintaining confidentiality of classified or privileged information.
- In closing, the information I am providing today is specific to your individual state and local government owned and operated election infrastructure, and includes operations that we assess were conducted at the behest of the Russian government. Specifically, I am only calling about cyber-related activities during the time period leading up to and directly after the 2016 elections.
- Having said that, it is important to note that malicious cyber activity, from both nation-state and criminal actors, has been directed at public and private sector networks involved in our electoral processes before 2016 and will almost certainly continue. That is why it's important that this dialogue continue and we create processes to ensure timely

communications, even in the absence of an acute threat.