Recommendation to the House Select Committee on the Modernization of Congress to bolster remote & district office technology for First Branch Continuity of Government (COG). 10/19

Lorelei Kelly, Director of Congressional Modernization, Beeck Center for Social Impact + Innovation, Georgetown University; Marci Harris, CEO, POPVOX; Maggi Molina, Demand Progress. Please email Lorelei.Kelly@georgetown.edu for follow-up.

The ability to receive and convey secure information is a constitutional imperative for Members of Congress and should be viewed with a national security lens.

The legislative branch — Members of Congress, staff, operations, and support agencies — conducts almost all of its business on the U.S. Capitol campus, with the notable exception of some 900 district offices across the country. This centralized physical organization may limit Congress' ability to effectively and securely function if faced with a catastrophic event that makes travel to or convening in Washington (or alternative sites) impossible or dangerous. **Congress should prioritize and secure its remote capacity and technology, leveraging its existing district office structure, to prepare for such an event.**

Existing legislative branch continuity of government (COG) planning is dated or based primarily on mass casualty scenarios.[1] However, a number of scenarios — from electro-magnetic disruptions, pandemics, or bio attack — might imperil the ability of Congress to physically convene, but need not bring the legislative branch to a standstill. Technology provides ample opportunity for secure, authenticated communication and legislative activity that would allow the first branch to continue to function even in an emergency that limits physical movement.

THE PROBLEM:

Congress has also not sufficiently planned for its continued operation if a physical convening of members is not possible. The distributed and disconnected architecture of Congress means that each office, to a certain extent, maintains its own communications technology, with wide variation of technical sophistication and security. While the U.S. Capitol Police has, in recent years, taken steps to better protect the physical safety of lawmakers while they are outside of DC, there has been much less focus on digital security and efforts to ensure secure connectivity for lawmakers in their districts.

THE OPPORTUNITY:

Upgrading and securing connective technology for Congress—including district offices and remote access for lawmakers—would ensure that the legislative branch would continue functioning in a disaster. It would have the additional benefit of improving overall district office security and communications functionality.

---

[1] The Continuity of Government Commission report, published in 2003 is important context. Also see CRS report RS21140 on Emergency Electronic Communications in Congress Issues & Legislative Proposals, 107th and 108th Congresses. Congress has two chambers. This memo is focused on the House.

RECOMMENDATIONS:

- Establish a task force to create a modern continuity plan for Congress, including an examination of best practices from state legislatures[2] and the Executive Branch
- Consider designation of district offices as "critical infrastructure"
- Ensure that district offices are included in "FirstNet" connectivity planning.[3]
- Develop an encrypted communications application for lawmakers and authorized staff with secure, verified log-in
- Approve a secure technology platform for House and district offices that includes the capacity to support secure remote communications systems
- Provide ability for district office staff to "report up" to a secure information hub their on-the-ground observations, critical rapid response notices and analysis
- Review if members have sufficient state staff with security clearances (and access to facilities to handle classified information)

ADDITIONAL CONSIDERATIONS

- Communications and Infrastructure
    - Do district offices have access to hardened and secure technology if commercial networks are down? (i.e. access to FirstNet)
    - What additional communications options exist?
    - What is the protocol for legislative branch updates in an emergency?
    - Are members/staff admitted to state and local emergency management HQs?
    - Are lawmakers included in executive branch briefings (regardless of party)?
- Ability to take action
    - If it is unsafe or not possible for lawmakers to physically convene in one location, is it possible for Congress to act?
    - How could lawmakers be verified to allow remote functions, such as additional uses for member voting cards, facial or voice recognition, "multi factor" authentication (*e.g.*, biometrics plus a physical verification by another member or authorized staff)
    - How would Congressional support offices (Clerk, Senate Sec, Parliamentarian, GPO, etc.) fulfill their functions remotely?
    - How can Congress maintain public information and appropriate transparency in an emergency?

---

[2] See Legislative Continuity of Government from the Natl Conference of State Legislatures

[3] *FirstNet is an independent authority within the U.S. Department of Commerce. Authorized by Congress in 2012, its mission to develop, build, and operate the nationwide, broadband network that equips first responders to save lives and protect U.S. communities.*