# TESTIMONY BEFORE THE HOUSE COMMITTEE ON ADMINISTRATION
# HEARING ON
# "EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE VOTING IN THE HOUSE"

**JON GREEN**
**CHIEF TECHNOLOGIST, CYBERSECURITY AND GOVERNMENT SOLUTIONS**
**ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY**

**JULY 17, 2020**

Chairwoman Lofgren, Ranking Member Davis, Members of the Committee, thank you for inviting me to testify as you explore the feasibility and security of remote voting for those of you serving in the House of Representatives. While recognizing that this institution is founded on in-person engagement and voting requirements, the current pandemic has created an unprecedented need to consider technology that allows for secure remote voting capabilities. I am the Chief Technologist for cybersecurity and government solutions at Aruba, a part of Hewlett Packard Enterprise (HPE), where I've spent the past 17 years. For the past ten years, I've worked closely with our US and allied partner government customers on secure network and remote access solutions, and I hope that experience will help me provide relevant information on today's topic.

Before beginning my formal testimony, I want to thank Chairwoman Lofgren for her representation of San Jose and Silicon Valley over the past 25 years. HPE and the larger technology community in the Valley are grateful for her consistent support and leadership. I also appreciate the hard work that the Members and staff of the House Administration Committee have done over the past four months to keep the House of Representatives up and running. A functioning legislative branch is critical to successfully addressing the ongoing pandemic, and alternatives for safe and secure voting should be a part of any plan.

As you may know, in 2015 Hewlett Packard Enterprise emerged from HP, an 80+ year old technology innovator in the United States, and you will find our IT products and services interwoven throughout organizations around the world. Based on our experience, I can assure you that you are not alone in trying to adapt to the new world of work-from-home orders. Since this pandemic began, we have received thousands of inquiries from our enterprise customers, both inside and outside the government, seeking solutions to enable secure remote working. The fortunate ones had begun remote working initiatives years ago and only needed to expand their existing footprint, but it's fair to say that very few of our customers had ever envisioned a world where 100% of their workforce would be working from home. Such widespread remote working brings with it additional challenges. End users, without the benefit of on-site IT support personnel, often become frustrated if their technology doesn't work the same way it does inside the office. And without protections provided by enterprise IT security solutions, users often turn to that which is convenient, such as personal email accounts, rather than that which is secure. The stakes are very high when it comes to remote voting in the House, so it is critical to provide Members a solution that is *both* convenient and secure.

In the world of information security, we often speak of the CIA triad. Not to be confused with a US intelligence agency, CIA stands for confidentiality, integrity, and availability – the three most important aspects of a secure system. Many people equate "security" with "confidentiality", but in remote voting the most important principle is actually *integrity* – the guarantee that information is trustworthy, consistent, accurate, and originated from the correct person. Second in importance is availability – the system must be highly reliable so that a Member is able to cast a vote during the period that voting is open. We have all seen the reports documenting foreign adversary interference in US public elections and we can't for a minute believe that adversaries would not also try to interfere in Congressional voting. For that reason, it is imperative that the House implement the highest degree of security possible, and consider backup options.

Fortunately, a model already exists for highly secure remote access; Congress does not have to go first. Since approximately 2010, I and other industry colleagues have worked closely with the National Security Agency on an architecture and program known as Commercial Solutions for Classified. This program has been widely used by the DoD, the intelligence community, the Department of Energy, law enforcement, and others to connect classified systems and devices over Wi-Fi networks, cellular networks, and the public Internet using commercial off-the-shelf information technology products. This same architecture has also been deployed for unclassified systems when organizations have needed to adopt the best security available. The Congress can dispense with months of security analysis by adopting an existing proven architecture, with reasonable modifications where necessary.

Overall, I believe we need to focus on four key principles to ensure a successful remote voting program:

- First, as previously mentioned, secure remote network connectivity should be provided using a layered approach that follows the NSA Commercial Solutions for Classified architecture. This ensures that Members of Congress are not connecting to malicious or compromised networks.
- Second, dedicated voting devices should be issued to each Member, to be used only for the purpose of voting. These could take the form of laptops, tablets, or smartphones. Some degree of system integration would be required to ensure these devices are as simple to use as possible, but we do not need complicated custom software. Because the network is secure, nothing more than a web browser is needed, with a simple application showing buttons labeled “Yes”, “No”, and “Present”.
- Third, multi-factor authentication (e.g. something you have + something you know) would be mandatory for such a solution. It is critical to ensure that the Member, and only the Member, is the person casting a vote. Multi-factor authentication is already widely

used by the Federal government in the form of smart cards and biometrics, and is a well-understood technology.

- Fourth, a manual system of vote verification is required, to counter against both concerns around central vote tallying systems and the threat of availability attacks. In public elections, concerns over electronic voting machines can often be alleviated through use of machines that instantly print a paper voting record for the voter to verify. In remote Congressional voting, the Member needs a way to verify that the correct vote was registered, in a system that is visible to all. This could be as simple as monitoring the vote on CSPAN or listening to a conference call line as voting results are read aloud.

My remaining caution to you is to focus on availability. We can solve for integrity and confidentiality, but availability is often overlooked in security. Systems deployed today that use the public Internet rely on users being “lost in a crowd”, their Internet traffic appearing indistinguishable from others. If an adversary were able to pinpoint the Internet location, or IP address, of each Congressional member, then targeted denial of service attacks could prevent specific members from casting their votes. To counter this threat, backup systems of voting must remain available and time limits on voting windows may need to be relaxed. As skilled as we are today at engineering reliable networks, the best backup systems are often non-technical.

In summary, I believe that should you decide to move forward, remote voting is technically feasible, can be enabled for a reasonable cost, and can be done with an appropriately high level of security. Once built, such a system can be easily modified should similar emergencies arise in the future to create the need for remote voting. Thank you again for the opportunity to offer testimony and I look forward to answering any questions you may have.