for all agencies involved. "The U.S. government is actually stronger if the whole resources and expertise of the interagency are brought to bear. [USAID] is an important part of that, but we're not the only part," said Warren.

When discussing USAID's role in the response to the 2014 Ebola epidemic, Warren said "I think if it had come 20 years earlier when we were less used to working in the interagency we would have struggled more." Instead, Warren counts the agency's role in the response effort among his most notable experiences with USAID.

Warren served as acting Administrator for several months prior to Administrator Green's confirmation. He also served in missions in Zimbabwe and Botswana, and held senior management positions in the Bureau for Global Health and the Bureau for Policy, Planning and Learning.

- DevEx

DHS releases new cyber strategy

In May the Department of Homeland Security (DHS) released their new cybersecurity strategy. The new cyber addresses the growing number of cyber threats and security risks, and provides DHS with a framework to execute their cybersecurity responsibilities during the next five years.

The new cyber strategy will focus on coordinating departmental cybersecurity activities to ensure a unity of effort, and outlines how DHS will leverage its unique capabilities to defend American networks and get ahead of emerging cyber threats. "The cyber threat landscape is shifting in real-time, and we have reached a historic turning point," said DHS Secretary Kirstjen Nielsen.

DHS's cyber strategy lays out a five-part approach to manage national cyber risk that fosters innovation, efficiency, communication, and economic prosperity.

- Risk Identification: Assess the evolving national cybersecurity risk posture to inform and prioritize risk management activities.
- Vulnerability Reduction: Protect federal government information systems by reducing the vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.
- Threat Reduction: Reduce national cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.
- Consequence Mitigation: Respond effectively to cyber incidents to thereby minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.
- Enable Cybersecurity Outcomes: Strengthen the security and reliability of the cyber ecosystem by supporting policies and activities that enable improved global cybersecurity risk management and execute departmental cybersecurity efforts in an integrated and prioritized way.

- Department of Homeland Security