**Continue Meaningful State CIO/CISO Participation in FEMA's Senior Advisory Committee and Urban Area Working Group**

> ***State CIOs have listed cybersecurity as their number one strategic priority in NASCIO's annual state CIO Top Ten priorities for the last six years.***
>
> ***In the 2017 Homeland Security Advisor (HSA) survey conducted by the National Governors Association, it stated "HSAs are extremely concerned about cybersecurity and consider it to be the single largest issue for states and the federal government. Many officials are very concerned about a potential cyberattack, but few consider themselves prepared to address this threat."***

Cybersecurity is a critical threat and business risk facing the nation. As state leaders and experts in information technology, state CIOs have a unique duty and responsibility to secure state government against digital threats. To that end, NASCIO supports continued and meaningful engagement of state CIOs and CISOs on state senior advisory committees (SAC) and urban area working groups (UAWG) which govern state homeland security program (SHSP) and the urban area security initiative (UASI) grants managed by the Federal Emergency Management Agency (FEMA).

In May 2018, the Federal Emergency Management Agency (FEMA) announced key changes in their FY 2018 Notice of Funding Opportunity (NOFO) and required states to develop a cybersecurity investment justification and include chief information officers (CIO) and chief information security officers (CISO) in the SAC and UAWG. The responsibilities of the SAC include: integrating preparedness activities across disciplines, creating a cohesive planning network, ensuring that SHSP and UASI funds align with capability gaps, and assisting in the preparation and revision of homeland security plans among others. The UAWG has similar responsibilities and is required to ensure that funding under the UASI program supports closing capability gaps identified through the threat and hazard identification process (e.g. THIRA).

The membership composition of both the SAC and UAWG include other members of state and local governments, health officials, non-profit organizations and others that can collectively contribute their expertise to develop a comprehensive view of the threats facing the community. In identifying current and future threats to state governments, state CIOs and CISOs can contribute cybersecurity threat data that can inform the THIRA process and lend expertise around cybersecurity response. In addition, NASCIO encourages cross-jurisdictional efforts focused on mitigating risks for the continuity of government. Reciprocal arrangements between governments for facilities, IT infrastructure and services may be appropriate starting points.