# Congress May Press DHS to Bolster Cybersecurity Workforce Development

Posted At : November 25, 2013 3:33 PM | Posted By : John Slye

Related Categories: Department of Homeland Security, Technology Trends, Legislation, Information Security, Congress, IT Workforce, Cybersecurity, Policy & Legislation

When we hear the phrase “boots-on-the-ground” most of us think of uniformed military personnel being deployed in active combat situations. But a current bill in the U.S. House of Representatives uses the phrase in connection with boosting Department of Homeland Security (DHS) efforts to improve its domestic cybersecurity workforce development activities.

In October, the **House Committee on Homeland Security** marked-up and passed the bill by voice vote authorizing it to be reported to the full House for consideration. It joins several other cybersecurity-related bills that have been introduced and are at various stages of progression. It is yet unclear which if any of these bills will progress to a vote in the House and are taken up in the Senate, given other priorities.

**HR 3107 - Homeland Security Cybersecurity Boots-on-the-Ground Act**

**The bill** in its current form would require DHS to develop:

- Occupation classifications for individuals performing cybersecurity mission activities and ensure that they are used throughout DHS as well as other federal agencies
- Workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the DHS cybersecurity workforce, including a multi-phased recruitment plan and a 10-year projection of federal workforce needs
- Verification process so that contractor cybersecurity employees at DHS receive initial and recurrent information security and role-based security training

Other provisos

- Defines "cybersecurity mission" as threat and vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace.
- Directs the DHS Chief Human Capital Officer and Chief Information Officer to assess the readiness and capacity of DHS to meet its cybersecurity mission.
- Requires the Secretary to provide Congress with annual updates regarding such strategies, assessments, and training.
- Expands recruiting outreach through a tuition-for-work fellowship program and a program to identify military veterans and unemployed computer specialists for potential DHS cybersecurity employment

**Implications**

The challenge that DHS has faced with recruiting and retaining cybersecurity personnel is not breaking news. DHS has announced multiple efforts to improve recruitment and retention over the last 5+ years. Even with those efforts, the **GAO reported** earlier this year that more than 20% of cybersecurity positions at the National Protection and Programs Directorate (NPPD) are vacant (see p. 24).

To cope with the shortfall agencies have continued to supplement their internal workforce with contracted personnel, but budget constraints from all sides add to the challenge. According to OMB, up to 90% of federal IT security spending is on personnel costs. The rest is a mix of training, testing, cyber tools and risk management policy implementation.

It seems to me that this is a tough cost model to sustain in an increasingly constrained fiscal environment, but the nature of current cybersecurity operations and existing needs present challenges to automating many functions that require experienced analysts’ eyes (or “boots,” to follow the theme) monitoring the networks. The nature of the work combined with the priority of improved overall cybersecurity continues to show growth prospects, bucking the budget belt-tightening trend.

Read more of our perspective in our latest report: ***Federal Information Security Market, FY 2013-2018***.

---
*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*