Will Congress Help DHS Stem its Cyber-Workforce Hemorrhaging?

Posted At : October 2, 2014 3:50 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Department of Homeland Security, Technology Trends, Intelligence Community, Homeland Security, Legislation, Information Security, Congress, IT Workforce, Cybersecurity, Policy & Legislation

Recent news media reports reveal endemic leadership and staff turnover and low morale at the Department of Homeland Security (DHS) and these challenges continue to impact both its intelligence and cybersecurity missions and the department's ability to attract and retain skilled experts. Now, it appears that some legislation in Congress might help address some of the issues.

According to a recent **Washington Post report**, over the past four years, federal employees have left DHS at a rate that is nearly twice as fast as the overall federal government, and the trend is accelerating. Morale is dismal, by most reports, and the department's ability to attract replacements and new talent has been slow and ineffective. Contributing factors include cultural clashes and in-fighting among the sub-agencies, bureaucratic lethargy, unclear missions, a high degree of regulatory oversight, and low pay compared to similar jobs in the private sector. The departures have hit the leadership area especially hard. The department's -top-level vacancy rate had reached 40 percent, although the Senate has confirmed 10 top DHS officials in the last six months or so.

The high-level leadership departures have hit hard DHS's intelligence functions as well as cybersecurity. The Post reports that between June 2011 and March 2012, four senior DHS cybersecurity officials left, right as DHS was arguing its case to Congress to be given more authority in protecting critical private-sector infrastructure and networks, a failed effort. High churn rates have also impacted operational areas like the **National Cybersecurity and Communications Integration Center** (NCCIC), which just recently lost its director and another key leader. The high turn-over rate is credited with stalling the progress of major programs like EINSTEIN. Compensation is a major issue as cybersecurity experts can make 2-3 times as much, or more, in the private sector than they can at DHS.

While numerous legislative bills aimed at beefing up the federal cybersecurity workforce have come and gone over the last few years, one effort to support DHS has gained legs recently. The Senate recently passed the **Border Patrol Agent Pay Reform Act of 2014**, which includes the **DHS Cybersecurity Workforce Recruitment and Retention Act** that is aimed at helping the department recruit and retain cybersecurity experts.

A **recent article** summarizes the provisions to include:

- Giving DHS greater hiring authorities, similar to those at DoD, to expedite the on-boarding of cybersecurity staff, as well as greater leeway in compensation,
- Requiring DHS to report annually on the progress of the hiring effort, and
- Requiring DHS to develop cyber- occupation classification codes for staff performing cybersecurity activities to aid in identifying and fulfilling its cybersecurity needs.

What gives some hope to the current Senate bill is that it is similar to the **Homeland Security Cybersecurity Boots-on-the-Ground Act** that passed the House this summer. **I discussed this House bill** when it first passed out of committee back in October, 2013. Now, nearly a year later, we will see if this or the Senate bill has enough legs to be passed as-is by the other chamber or can survive a conference committee mark-up and re-vote in both chambers to make it to the president. Given that we are in a Congressional election year with little left in the legislative calendar before the run-up to November, such fate may fall to the lame duck session and that is an uncertain fate for sure.

Even if legislation were enacted immediately, it will take significant time to for DHS to make up lost ground and build up its workforce. Until then, they look to industry to help fill the gaps and protect the department and the rest of the .gov domain from an increasingly hostile cybersecurity landscape.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@GovWinSlye**.*