Cyber Security Training:

Name:

Institution Affiliation:

Training is very important in preparation of the cyber security workforce of tomorrow. It enhances the workers remain up-to-date concerning the skills required and concerning the threats that are evolving (Busch Givens 2012).. Department of Homeland security provides the country with access to cyber security training and development of the workforce to ensure there is a more resilient country and that there is a capable cyber nation. Cyber space is exposed to a wide range of risks which stem from not only physical threats but also cyber threats and hazards. Cyber actors take advantage of these treats to disrupt, destroy and make the delivery of important services difficult.

A program known as Homeland security exercise and evaluation program (HSEEP) is responsible for providing principles which guide the department, evaluate en improve the planning. It is through this program that managers can develop and evaluate the activities identified by the leaders.

Withdrawal from Iraq and partial withdrawal from Afghanistan has made the largest traditional defense efforts of the year 2014 (Busch Givens 2012). Currently, the department has over two hundred and forty thousand employees. It has cooperated with over twenty two agencies. However, this department has been ridiculed over years over its disorganized nature. It is also said that it is unwieldy and that it is a source of waste. It has however tried to clean its image over the years. The greatest areas that the department is trying to improve includes complying with the government, they have also tried to work on their transparency. They have tried to fix the immigration system and also they have come up with better measures to counter terrorism activities.

Currently the department has worked on their information technology and cyber security. In the year 2010, it was reported that the department has continued to strengthen their security programs. The department has implemented a plan that would improve on four key areas. That is, plan of action and milestone, weakness remediation, quality of certification and accreditation, annual testing and validation and security program oversight.

All professionals in homeland security at all levels are required to undergo through training inform of practicum, classroom and on the job training (Busch Givens 2012). This helps all the professionals to internalize the most essential principles, procedures and activities in their area of specialization. Instructors are usually professionals who have years of experience, and academic qualifications attained after a rigorous course of study.

Training programs are offered at different levels. One that is called in-service training is done before one has been fully employed. It equips people with knowledge and experience within their area of specialization. It is within this period that orientation is done to familiarize the in-service people with the day to day operations of the department. In service training serves two main purposes. First, it provides advanced knowledge on new concepts and practices developed after the first training (Busch Givens 2012). It is a requirement for almost all organizations in homeland security that all professionals participate in In-service training during their career period because of the rapid changes which are there. This helps the professionals to be up to date concerning whatever is in the nation because the current world is very dynamic. Failure to keep training may make the professionals to rug behind which would make their activities difficult out of dealing with terrorists who might have a lot of knowledge concerning information technology.

There is a federal level training which is the lead agency for homeland security at the federal level. This is the department of homeland security (DHS). It is responsible for all the professionals at all levels of the government and partly on private sector. It has training facilities which include center for domestic preparedness. This body is responsible for providing training to local and state emergency responders who have weapons of mass destruction. There is also a center known as energetic materials and research testing center. It gives information to teams concerned with bombs. It equips them with knowledge on bomb neutralization, removal of the same and analysis of bombs (Busch Givens 2012). This has enabled the homeland department to have high knowledge on bomb neutralization and all the deals concerning bombs have been dealt with. There is also a center for biomedical research and training. This center offers more than twenty five courses to emergency medical responders as well as to ten online courses. It is therefore equipped with matters concerning medical issues and incase of any issue that has emerged concerning medicine it can be dealt with amicably.

There is also a national disaster preparedness training centre. This center is responsible for provision of remedial actions in case of a disaster occurring in coastal and island communities. It therefore ensures there is enough security and that incases of any disasters along the coast and island communities they can be dealt will in the right manner and without wasting time. Other centers include, counter terrorism operations support, national emergency and rescue training center among others.

Finally, there is a state level training. The federal government provides the guidelines for training, resources required for training but the states are the ones that provide specific training regime for homeland security professionals in the state. Programs take into consideration the state of that region as states are different. Characteristics of each state are taken into consideration to ensure that there is effectiveness in service delivery. Training programs, though different, incorporate the same standards of effectiveness which are required in the entire country. This ensures the effectiveness of cyber security training at the department of homeland security.

References

Busch, N. E., & Givens, A. D. (2012). Public-Private Partnerships in Homeland Security: Opportunities and Challenges. *Homeland Security Affairs*, *8*(1).

Kessler, G. C., & Ramsay, J. D. (2014, January). A proposed curriculum in cybersecurity education targeting homeland security students. In *2014 47th Hawaii International Conference on System Sciences* (pp. 4932-4937). IEEE.

Lewis, T. G. (2014). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), 583-594.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Yet, A. W. S. (2005). Homeland security.