Cybersecurity profile on the cia

CIA Cybersecurity Profile Table of Contents AC SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES 3 RA-2. SECURITY CATEGORIZATION 3 PM-2. SENIOR INFORMATION SECURITY OFFICER3

PL-2 (2). SYSTEM SECURITY PLAN4

PS-3. PERSONNEL SCREENING4

References4

AC-1. SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

The CIA develops and documents security awareness and training policy and procedures, evident from its intensive focus on security issues tied to emerging IT and communication platforms, including the Internet (Clift, 2007). There is not enough data to assess whether such procedures address roles and responsibilities, scope and purpose, but the assumption from the wealth of evidence suggests rigor, and so it may be assumed that such is being addressed. The same goes for the dissemination of documented procedures for those with roles related to them, and the formal development of those procedures (National Institute of Standards and Technology, 2010, pp. G-1 – G-2, F-51; National Archives and Records Administration, 2000; Central Intelligence Agency, 2012).

RA-2. SECURITY CATEGORIZATION

The available data suggests that the CIA strictly categorizes data and information systems in accordance with the laws, directives and guidelines attendant to the critical nature of the work of the CIA and the confidential nature of such data and systems. The data suggests formal documentation, as evident from the rigor of the categorization, though formal documentation is not available from the sources. The assumption is that categorization approval is embedded in the CIA policies and procedures, and emanates

from the very top of the organization (National Institute of Standards and Technology, 2010, pp. G-1 – G-2. F-226; Clift, 2007; Clift, 2007; Thibodeau, 2009).

PM-2. SENIOR INFORMATION SECURITY OFFICER

The CIA does appoint a senior information security officer to take charge of information security program coordination, development, implementation and maintenance across the whole organization, in the person of the Chief Information Officer or CIO. The CIO is empowered with the appropriate mandate, coming from the US President and the organization, as well as with the appropriate resources for the purpose (National Institute of Standards and Technology, 2010, pp. G-1 – G-2 , F-207, Office of the Director of National Intelligence, 2012).

PL-2 (2). SYSTEM SECURITY PLAN

From the available literature, and from the example of its evolving cloud architecture, the functional architecture exists with the corresponding external interfaces, the appropriate security clearances and levels, information storage and transmission compliant with the laws, and level of priority for restoration of the information and related services (National Institute of Standards and Technology, 2010, pp. G-1 – G-2, F-201; Clift, 2007; Central Intelligence Agency, 2012; Thibodeau, 2009).

PS-3. PERSONNEL SCREENING

There are appropriate screening procedures prior to access to information systems, as is evident in the current literature on the CIA initiatives on the Internet, including the cloud. The existing literature though, does not have data on re-screening, and it is not easy to extrapolate such details from the available data (National Institute of Standards and Technology, 2010, pp. G-1

– G-2, F-219; Clift, 2007; Central Intelligence Agency, 2012; Thibodeau, 2009).

References

Central Intelligence Agency (2012). Counterintelligence. CIA. gov. Retrieved 27 September 2012 from https://www. cia. gov/library/reports/archived-reports-1/ann_rpt_1999/dci_annual_report_99_16. html

Clift, A. (2007). Intelligence in the Internet Era: From Semaphore to Predator. CIA. gov. Retrieved 27 September 2012 from https://www. cia. gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article06. html

National Archives and Records Administration (2000). Records Management in the Central Intelligence Agency. FAS. org. Retrieved 27 September 2012 from http://www. fas. org/sgp/othergov/naracia. html

National Institute of Standards and Technology (2010). NIST Special Publication 800-53A Revision 1: Guide for Assessing the Security Controls in Federal Information Systems and Organizations- Building Effective Security Assessment Plans. US Department of Commerce. Retrieved 27 September 2012 from http://csrc. nist. gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final. pdf

Office of the Director of National Intelligence (2012). Chief Information Officer. DNI. gov. Retrieved from http://www. dni. gov/index. php/about/leadership/chief-information-officer

Thibodeau, P. (2009). CIA building secure cloud-based system. Computerworld. Retrieved 27 September 2012 from http://www. computerworld. com/s/article/344455/CIA_Building_Secure_Cloud_based_System