

Select Five Number SF0073

Requesting Entity Name Office of MN.IT Services

Request Title BCA Security Vulnerability Assessment

Request Description
 BCA MNJIS Vulnerability Assessment (VA) Statement of Work 1. Penetration Testing - External (Public) and the State s Criminal Justice Data Communications Network (CJDN) Scope - Perform an assessment on all assets accessible frOm the Internet (Public) and CJDN. - Perform an assessment on all assets accessible frOm the State s Criminal Justice Data Communications Network (CJDN). - Number of Active/Live IP addresses: Approximately 2,800. - Number of externally facing public web applications: o 35 sites accessible frOm the CJDN o 9 site publicly accessible 2. Internal Network Vulnerability Assessment Scope Conduct security testing to assess one (1), host and service discovery, and two (2), vulnerability identification and verification. Host and service discovery compiles a complete list of all accessible systems and their respective services with the goal of obtaining as much information about your internally facing assets as possible. This includes initial live host detection, service enumeration, and operating system and application fingerprinting. In particular, the discovery process will focus on identifying critical assets and major technologies in the environment such as Active Directory, ACS, and critical applications and databases. - Approximate number of hosts (servers, desktops and laptops): 400 servers (physical + VM) + 575 desktops and laptops - Approximate number of network devices (switches, routers, firewalls, printers, and storage devices): o 90 printers o 75 switches, routers, firewalls, and storage devices 3. Application Penetration Testing Web Applications and Web Services Scope Identify both common and application specific vulnerabilities using both unauthenticated and authenticated/credentialed scanning and assessment procedures. Authenticated testing will use credentials to the application using the roles of normal users to determine if valid users can exploit vulnerabilities to gain access to the underlying infrastructure or to information the user is not authorized to access. For role-based systems, testing will be conducted across all user roles not to exceed 3 roles. Number of authenticated applications: Approximately 30. Number of user roles: Varies by application. Not to exceed 5 for any one applications. 4. Deliverables Upon completion of the assessment, the vendor shall provide an electronic report deliverable. The report will provide an analysis of the current state of the assessed security controls. The analysis will identify areas that need to be resolved in order to achieve an adequate level of security. The detailed contents of the deliverable are described below. The report deliverable will include the following high level sections in a format suitable for management: Purpose of the engagement including project's scope and approach Positive security controls that were identified Tactical resolutions to immediately reduce risk in the environment Strategic recommendations for preventing similar issues frOm recurring An industry comparison based on consultancy experience and results frOm similar previous engagements The report deliverable will also include the following in-depth analysis and recommendations for technical staff to understand the underlying risks and recommendations: A technical description and classification of each vulnerability Business or technical risk inherent in the vulnerability Vulnerability classification that describes the risk level as a function of vulnerability impact and ease of exploitation Technical description of how to mitigate the vulnerability.

Contract(s) Awarded

Contract ID 105788

Entity Type

State Agency

Information on contracts executed by an entity type of State Agency can be found using the contract ID in the MN Open CheckBook under TransparencyMN located at <http://mn.gov/mmb/transparency-mn/>.

For information on contracts executed by an entity type other than State Agency you will need to contact that entity directly using the contact information that was provided in the Select Five.