**INFORMATION SYSTEMS SECURITY PROGRAM**

**Department of Controlled Substances**

**FYE December 31st, 2015**

# This audit program covers the security over the information systems of the Department of Controlled Substances (DCS). A description of critical agency systems, security controls, and information system structure is documented in the following narrative. These systems support the processes described in the other audit programs comprising this entire audit project.

# The test procedures in this program support the systems security test objectives well as the audit objectives outlined in the program. However, it does not test all internal controls built into information systems used by the Department of Controlled Substances (DCS). System controls that provide for things such as data accuracy and completeness (application controls) should be addressed in the appropriate business process audit program.

## Step 1: Narrative

Provide the detailed narrative of the Agency’s or Institution’s IT Environment as it relates to the audit objectives and financial assertions of the general audit program. Document the internal control processes as they relate to the confidentiality, integrity, and availability of information.

**Step Completed by & Date:** [Group 3 & 04/26/2017]

**Step Reviewed by & Date:** [Insert Name & Date]

**CONTACTS**

Chuck Ross Chief Information Officer

rosscd@vcu.edu 804.XXX.XXXX

Matt Robinett Chief Information Security Officer

robinettmw@vcu.edu 804.XXX.XXXX

**NARRATIVE**

The IT Narrative can be found embedded in the attached document, labeled “DCS IT Narrative.docx”.

[EMBED DOCUMENT]

## Step 2: Scope

Document the scope limitations for this particular project. Be as specific as possible when describing particular systems. Please list specific system names, platforms, and the applications they support. Also, document the reasoning for the scope of this particular program. Include how compensating controls will be evaluated in the absence of documented policies and procedures, or whether a management point is warranted.

*In my opinion, based on the agency’s procedures described above and an evaluation of their internal control structure, the audit procedures listed below are adequate.*

**Group sign/date:** Group 3, 04/26/2017]

**Project Manager sign/date:** [Matt will sign off, and Date]

**SCOPE**

1. **External Network Firewall:** Public-facing networking device, it remains a single point of failure for the Consumer/Sales system and its related system components and business processes. As such, it is the most critical firewall in the DCS network due to it guarding sensitive customer data such as PII, PCI, inventory, and logical information. A compromise of this firewall can result in loss of sensitive information, the ability to conduct mission critical business processes, upkeep time, and loss of revenue.
2. **Security Awareness & Training:** Recent reviews revealed that only 40% of employees have completed timely training. Improper awareness and training of employees can lead to a leakage of sensitive information, further compromise of the organization, and a loss of revenue.

These reviews should give reasonable assurance over core components of the DCS IT environment and help support the conclusions reached in the financial statement audit performed by the financial auditors.

## AUDIT PROCEDURES

## Step 3: Planning

A. Document the discussions and meeting that took place to derive your scope. Include class sessions with instructors, emails/conversations directly with instructors and your cohorts, industry research, and risks you noted in the DCS IT Narrative.

B. Prepare the *DCS Case Study* Excel document and embed it in the planning section.

**Step Completed by & Date:** [Group 3, 04/26/2017]

**Step Reviewed by & Date:** [Insert Name & Date]

* **March 1st, group 3 reviewed the DCS IT narrative.**
* **March 5th, Group 3 began the Planning phase the IT audit and completed the Preliminary Risk Assessment (Step 4).**
* **March 15th, Group 3 started the business line breakdown.**
* **March 18th, Group 3 started to begin reviewing the DCS Audit Scope Declaration and deciding which general controls would be appropriate for the Audit of DCS.**
* **Group 3 noted that one critical general control that needs to be looked into further is the external network firewall if compromised this firewall could result in a loss of sensitive data, the ability of employees to make orders, and customers to make purchases, resulting eventually into a loss of revenue.**
* **March 22nd, Group 3 noted another general control to further look into which is DCS security and awareness training. We found out that only 40% of the employees took the IT Security Awareness & Training session as required by their policy. .**
* **March 29th, Group 3 finished the DCS Audit Scope Declaration and determined two critical general controls to audit; DCS’s security and awareness training and DCS’s external network firewall. Additionally, group 3 sent an evidence request for DCS’s security and awareness training policy and DCS external network firewall.**
* **April 5th, Group 3 received the evidence request and begin reviewing the document in evidence request.**

## Step 4: Preliminary Risk Assessment

Considering the audit risk, fraud risk, internal controls, determine and document the following risks and the supporting information for the system security process:

\*Control risk is the risk that an error could occur in an audit area, and which could be material, individually or in combination with other errors, but the internal control system will not prevent or detect and correct the error on a timely basis.

**Step Completed by & Date:** [Group 3 03/05/2017]

**Step Reviewed by & Date:** [Insert Name & Date]

**PRELIMINARY RISK ASSESSMENT**

Auditor determined that the preliminary control risk is***high****.*

After reviewing the IT Narrative and Scope documents, Group 3 has determined that the preliminary control risk is high. We noted the following deficiencies in DCS general controls IT Systems/Data Backup and Restoration, IT Systems and Data Security, IT Security Awareness & Training, Logical Access Controls, IT Change and Control Management, Firewall Security, VPN Security, C/S Oracle Database Security, C/S Web Application Review (WIMS), and IT Risk Assessment.

## TEST WORK

While the Confidentiality, Integrity, and Availability of information relating to financial statements are maximized through a mature Information Security Program and the concept of “defense-in-depth”, that is, there is an exponential relationship between the layers of information security controls in place to the level of protection achieved; the audit test work in this program is focused and based on the identified risks above.

## Step 5: Security & Awareness Training

**Contacts** (Name, Title, and Contact info):

Chuck Ross Chief Information Officer

rosscd@vcu.edu 804.XXX.XXXX

Matt Robinett Chief Information Security Officer

robinettmw@vcu.edu 804.XXX.XXXX

**Step Completed by & Date:** [Group 3 & 4/13/2016]

**Step Reviewed by & Date:** [Insert Name & Date]

**Conclusion:** After reviewing the Security and Awareness Training policy and procedures and all the documents to go with it, Group 3 determined during fieldwork that DCS doesn’t have a separation of duties policy or anything in regards to separation of duties. Furthermore, Group 3 found that additionally in regards to access controls, that DCS doesn’t have such a policy. There is no policy that mentions access controls including creating and changing passwords. Also Group 3 noted that DCS doesn’t have any information about remote access in any of their policies, as well as no policy in place for intellectual property rights. Group 3 noted that all DCS employees receive the same security and awareness training regardless of their role and level of expertise. Additionally Group 3 noted that there is no designated individual to monitor and maintain signed acknowledgement forms of Security and Awareness Training. Lastly, Group 3 noted that no technical security training is provided for all individuals involved in information resources.

**Deemed Not Reasonable- See Observations “Security and Awareness Training”**

**Step 1: (Policy Existence)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Yes | No | N/A |
| A. | Does the Agency have a documented Security Awareness and Training Program Policy & Program? | X |  |  |
|  |  |  |  |  |

**Step 2: (Policy Completeness)**

Obtain and review the Agency’s IT Security Awareness and Training Policy and Program and determine whether it requires:

1. The development of a Security Awareness and Training Program so that each IT system user is trained in regards to the following concepts:

1) General Concepts to include

a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;

b. The concept of separation of duties;

c. Prevention and detection of IT security incidents, including those caused by malicious code;

d. Proper disposal of data storage media;

e. Access controls, including creating and changing passwords and the need to keep them confidential;

f. Agency acceptable use policies;

g. Agency Remote Access policies; and

h. Intellectual property rights, including software licensing and copyright issues.

a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data

Auditor Camper reviewed the document DCS Internet and acceptable use policy in the section labeled protecting information and shared documents.doc, on page 2, bullet point 4. The document states “Not to copy or save sensitive data to mobile or removable devices including, but not limited to laptops, iPads, smart phones, CDs, DVDs, USB drives, external hard drives (unless encrypted and authorized by the CEO).”

Deemed Reasonable

b. The concept of separation of duties

Auditor Camper reviewed all of DCS security and awareness training documents and found that DCS has no concept of separation of duties. Auditor Camper sent a evidence request to verify whether or not DCS has any policies regarding separation of duties and DCS on 04/12/2017. DCS replied back on 04/12/2017 to inform the Audit group they had no such policy regarding separation of duties.

Conclusion Deemed Not Reasonable, Improve Security and awareness training

c. Does DCS have a prevention and detection of IT security incidents, including those caused by malicious code?

Auditor Camper reviewed the document DCS Internet and acceptable use policy.doc in the section labeled proper use of resources, on page 2 under the section “Proper Use of Resources”. Additionally, Auditor Camper found that DCS requires that all laptop devices have firewall protection installed on the system which is found in the document DCS Electronic Media Policy on page 2 of the policy section under, laptops

Deemed Reasonable

d. Proper disposal of data storage media

Auditor Camper reviewed the document DCS Electronic Media Policy.doc in the section called “policy”. Subsection A starting on page 1, states that no one besides the ITO staff should dispose of any DCS hard drives, prior to disposing a DCS computer you must remove the hard drive, and all DCS hard drives must be physically destroyed and to never be recycled. Subsection B of the policy section on page 2, states that all laptops may only be disposed of only by the ITO staff. Likewise, for all forms of removable media must be given to the ITO staff so they can properly dispose of the media.

Deemed reasonable

e. Does DCS access controls, including creating and changing passwords and the need to keep them confidential?

Auditor Camper, reviewed the document DCS Internet and acceptable use policy.doc in the section labeled “Authorized Use” on page 1. DCS states that users’ of the system cannot give out their user information. Additionally, in the section called “protecting information and shared resources” the document states that users have actively manage their passwords. Auditor Camper sent a evidence request to verify whether or not DCS has a policy in place for access controls, including creating and changing passwords and the need to keep them confidential, on 04/12/2017. DCS replied back on 04/12/2017 to inform the Audit group they had no such policy regarding access controls, including creating and changing passwords and the need to keep them confidential.

Conclusion Deemed Not Reasonable, Improve Security and awareness training

f. Agency acceptable use policies

Auditor Camper, reviewed the client audit response from DCS which include a document called DCS internet and acceptable use policy.doc which listed all acceptable uses of DCS agency devices

Deemed reasonable

g. Agency Remote Access policies

Auditor Camper, reviewed DCS’s security awareness and training documents and noted that in none of the documents does inform users about the remote access policy

Conclusion Deemed Not Reasonable, Improve Security and awareness training

h. Intellectual property rights, including software licensing and copyright issues

Auditor Camper reviewed all of DCS security awareness and training documents and found no policy or procedure on how to protect DCS intellectual property. Additionally, Auditor Camper sent a evidence request to verify whether or not DCS has a policy in place for intellectual property rights, including software licensing and copyright issues, on 04/12/2017. DCS replied back on 04/12/2017 to inform the Audit group they had no such policy regarding intellectual property rights, including software licensing and copyright issues.

Conclusion Deemed Not Reasonable, Improve Security and awareness training

2) Position appropriate security awareness content (i.e. positions affected by HIPAA, FERPA, PCI; data owner; system owner)

Auditor Camper reviewed DCS IT Security Awareness and Training policy and noted regarding evidence of additional training for specific positions dealing with sensitive customer data. That all DCS employees received the same security and awareness training regardless of their role. Additionally, those employees who are privileged users are expected to use their institutional and degree knowledge in lieu of supplementing additional knowledge.

**Deemed Not Reasonable**

1. IT security training before (or as soon as practicable after) IT system users receive access rights to the agency’s IT systems and annual refresher training in order to maintain these access rights. Implementation of a process to monitor and track completion of IT security training.

Auditor Camper reviewed DCS Information Security Awareness Policy document. In the Information Security Awareness Program, Section 1 states that anyone who uses DCS-owned systems, network equipment, or computer equipment, must read and sign the DCS Internet and Acceptable Use Policy before any system or network access is granted. New employees are given a chance to ask questions about this document during the Information Security Awareness Training. Information Security Awareness Training is mandatory for all new employees and performed annually during the employee review period.

**Deemed Reasonable**

1. Designate an individual who is responsible for all aspects of an agency’s security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

Auditor Camper reviewed DCS IT Security Awareness Policy and found that the Chief Information Security Officer (CISO) is responsible for developing the Security Awareness Program. Supervisors and Managers are responsible for ensuring that employees under their supervision have access to information security resources and they are compliant with the aforementioned policies and procedures. The CISO is responsible for keeping this policy current.

**Deemed Reasonable**

1. All IT system users, including employees and contractors, receive IT security awareness training annually or more often as necessary.

Auditor Camper reviewed the document DCS information security awareness policy.doc, and noted that all employees participated in mandated DCS security and awareness training. on page 2 subsection 3 in the information security awareness training is required to be administered to new and current employees. Additionally the IT security and awareness training is administered annually.

Deemed reasonable

1. Provide additional role-based IT security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate and design IT systems, i.e.
2. System Owners, Data Owners, and System Administrators,
3. IT Disaster Recovery team members, and
4. IT security Incident Response Team members.

Auditor Camper reviewed the DCS Audit Response - IT Security Awareness Training.doc and noted in the evidence request in section 4, regarding evidence of enhanced/additional training for privileged individuals involved in managing, administering, designing, developing, implementing, and/or maintaining information resources. That all DCS employees received the same security and awareness training regardless of their role and those employees who are privileged users use their institutional and degree knowledge to supplement additional knowledge. Employees institutional knowledge does not supplement additional training for specific IT role- based jobs.

Deemed Not Reasonable

1. The ISO (or designated individual) monitors attendance and maintains signed acknowledgement forms.

Auditor Camper reviewed DCS Audit Response Document and in Section 2 found the DCS Employee Listings Document of when DCS employees signed security acknowledgement forms. However after reviewing IT Security Awareness Training doc, Auditor Camper determined that there is no such policy in place that designates an individual to monitor attendance and maintain signed acknowledgement forms. There is a policy in place that says the CISO is responsible for developing an Information Security Awareness Program, but nothing about maintaining signed forms.

**Deemed Not Reasonable**

**Step 3: (Procedural & Control Implementation)**

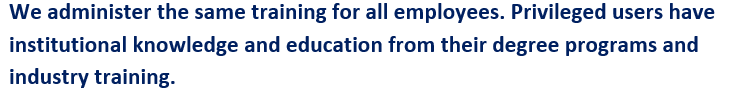
1. Determine whether security awareness training or a security awareness refresher training is provided to all employees and contractors at hire and annually thereafter and if the Agency maintains signed acknowledgements.

Auditor Camper reviewed the DCS Information Security Awareness Policy and Program document. Auditor noted that Information Security Awareness Training is mandatory for all new employees and performed annually during the employee review period. After reviewing DCS Employee Listings.xlsx file. Auditor reviewed DCS Employee Listing document determined that security awareness and training was not taken by all employees and contractors. All employee are responsible and must take the training annually.

Deemed Not Reasonable

1. Determine whether technical security training is provided for all individuals involved in managing, administering, designing, developing, implementing, and/or maintaining information resources.

Auditor Camper requested evidence that training was provided for all individuals in managing, administering, designing, developing, implementing, and/or maintaining information resources. Auditor received the evidence as showing below, and noted that all employees receive the same training regardless of job title. DCS does not provide enhanced training.



Deemed Not Reasonable

## Step 6: External Network Firewall

**Contacts** (Name, Title, and Contact info):

Chuck Ross Chief Information Officer

rosscd@vcu.edu 804.XXX.XXXX

Matt Robinett Chief Information Security Officer

robinettmw@vcu.edu 804.XXX.XXXX

**Step Completed by & Date:** [Group 3, 04/26/2017]

**Step Reviewed by & Date:** [Insert Name & Date]

**Conclusion:** After reviewing all of the DCS Audit Response documents to the Firewall for External Network, including the Juniper NetScreen DCS Security Report document, Group 3 has determined that DCS does not have vendor supported firewall system software. The operating system DCS is currently running id Juniper OS 6.2. This operating system has not been supported since 2005. Additionally, after consulting with DCS Group 3 determined that DCS does not have a policy in place or definite plan regarding patches, but administer patches as they become available. Group 3 also noted that DCS does not have a policy in place implementing patches to their firewall, and that DCS that they deliver patches as they become available. This policy is important to have, since the Juniper OS that DCS uses is no longer being supported by Juniper.

**Deemed Not Reasonable- See Observations “External Network Firewall”**

1. Evaluate the placement of the device in the network for segmentation purposes. Determine whether the placement is reasonable.

Auditor Camper reviewed the DCS Network Diagram in the DCS IT Narrative document and determined that the firewall is placed in the external network protecting the WIMS and POS applications. These two applications contain sensitive data. The placement of this is understood.

**Deemed Reasonable**

1. Determine if the firewall system software is vendor-supported and patches are current. Determine if a process exists to apply patches.

Auditor Camper reviewed the client audit response document and noted that in section 1 called the 1. Current firewall software version., DCS is running Juniper OS 6.2, which hasn’t not been supported since 05/15/2005, Additionally, after looking at the Firewall for External Network and Juniper Netscreen DCS security report.doc to find if they implement patches to the system Auditor Camper came back with no findings regarding implementation of patches and upon further review. Auditor Camper sent an evidence request to verify if they have a policy regarding implementation of patches and they said no they do not have a definitive plan on installing patches but they do administer patches as they become available. Auditor Camper sent an evidence request to verify whether or not DCS has a policy in place implementing patches to the firewall, on 04/14/2017. DCS replied back on 04/14/2017 to inform the Audit group they deliver patches as they become available. This process is not acceptable due to the current firewall being no longer being supported by Juniper.

**Deemed Not Reasonable**

1. Determine who has access to update the firewall configuration file and if that access is documented, approved, and reasonable. Determine if each administrator has individual admin accounts.

Auditor Camper reviewed the Firewall for External Network.doc and found that the access to the firewall configuration file is controlled through Logical Access policies and is executed by active directory permissions. The document had a list inside provided by DCS of specific employees who have access to this firewall configuration file.

**Deemed Reasonable**

1. Obtain a copy of the agency’s/institution’s latest vulnerability scan and determine if action was taken against critical items.

Auditor Camper reviewed the Firewall for External Network.doc and found that DCS does not scan for or take action against vulnerabilities due to the affects it has on the WIMS application the firewall protects. This leaves their firewall vulnerable to malicious users.

**Deemed Unreasonable**

1. Determine if communication is encrypted over the network when administering the firewall so that authentication data is protected.

Auditor Camper reviewed the Firewall for External Network document and found that the SSH protocol provides complete encryption of the network packets between the connecting client and the server. Section 3.4.3 of the Juniper NetScreen DCS Security Report Document is where Group 3 found evidence of the SSH connections .

**Deemed Reasonable**

1. Determine if the agency/institution requires, performs, and documents periodic connectivity monitoring. Determine if the agency follows-up on suspicious activity.

Auditor Camper reviewed the Firewall for External Network document and found that in section 5 labeled Connectivity Monitoring, the DCS informed the auditor that they do not scan for vulnerabilities because the scan will break the WIMS application it protects.

**Deemed Not Reasonable**

## Step 2 – Vulnerability Scanner Report Review

**Objective:**  
*A vulnerability scanner is used to automatically identify weaknesses in the firewall’s configuration file as compared to industry best practices.*

**Control:** *An automated vulnerability scanner is periodically used to test and identify weaknesses in the firewall configuration files used by the agency/institution.*

**Step Conclusion:**After using the vulnerability scanner and reviewing the Juniper NetScreen DCS Security Report document and other documents pertaining to the Firewall for the external network, Group 3 has determined that the current operating system version that DCS is using for their external firewall network is out of date. DCS is using Junos 6.2 which hasn’t been supported since 2005 (the most recent version of Junos is 17.1). Group 3 also noted that the vulnerability scanner found two “critical” findings; however after consulting with DCS, group 3 found that these findings were false positives. Furthermore, Group 3 noted that the vulnerability scanner found one other “high” finding in its report. Group 3 determined that the Telnet system does provide encryption or encoding. DCS reported to Group 3 that they use this service because of a vendor's technical limitations, and have asked them to change services, but cannot force them to do so.

**Deemed Not Reasonable- See Observations “External Firewall Network”**

**Step Completed by:** [Group 3, 04/26/2017] **Step Reviewed by:** [Reviewer’s name], [Date]

**Firewall Vulnerability Scanner Report Review**

1. **Firewall Operating System**

Determine what version of the operating system the firewall is running and compare the reported version to the most current vendor version.

Auditor Camper, reviewed DCS’s current firewall operating system and noted that on the DCS Audit Response - Firewall for External Network.doc under the section Current firewall software version and noted that DCS is currently running junos 6.2 which hasn’t been supported since 05/15/2005 and the most recent version of Junos is 17.1.

**Deemed Not Reasonable**

1. **Critical Findings**

*Examine all critical findings that are listed in the Firewall Vulnerability scan.*

List all findings labeled “Critical” by the Vulnerability Scanner. Provide the agency’s response to these findings and determine if they are false positives or actual findings.

Auditor Camper reviewed the Juniper Netscreen DCS Security Report and found the following “Critical” findings:

1.) In section 2.2 of the Juniper NetScreen document, Nipper determined that two rules allowed access between entire network address source and destinations with relaxed source port and destination services. A weak policy list configuration could allow a malicious user to gain unauthorized access. When Auditor Camper asked DCS about these two rules, DCS informed Auditor Camper that the two rules were part of their X11 service, which allows machines already on the network to talk to any other machine on the same network. These two rules are necessary for DCS business purposes. DCS does not believe the two rules present a risk to the organization, because these rules allow traffic only on the internal portion of their network. After consulting with DCS Group 3 has determined that these are false positives.

**Deemed Reasonable**

2.) In section 2.3 of the Juniper NetScreen document, Nipper determined 14 rules that allow access from any source address to any destination address and service. With a weak network filtering, the DCS external firewall would not prevent access to the network address and services detailed in the finding. These are actual findings, not false positives. Like the critical finding above, when Auditor Camper emailed DCS about these findings, DCS responded by stating that these rules provide for peer-to-peer networking for on-network machines and do not provide external access via LAN and Zone distribution of the internal networks After consulting with DCS Group 3 determined that these findings were false positives.

**Deemed Reasonable**

1. **High Findings**

*Examine all high findings that are listed in the Firewall Vulnerability scan.*

List all findings labeled “High” by the Vulnerability Scanner. Provide the agency’s response to these findings and determine if they are false positives or actual findings.

Auditor Camper reviewed the Juniper Netscreen DCS Security Report and found that section 2.4 Clear Text Telnet Service Enabled was a high finding during the Firewall Vulnerability scan. The Telenet is used to provide remote command based access to a variety of devices and is commonly used on network devices for remote access. The protocol provides no encryption or encoding. Nipper determined that the Telnet service was enabled on DCS-LL-D-FW01. An attacker or malicious user who was able to monitor the network traffic between a Telnet server and client would be able to capture authentication credentials and any data. When Auditor Camper emailed DCS about this finding, DCS replied by stating that they use Telnet because of an external vendor that requires the use of Telnet to send orders. This is due to the vendor’s own technical limitations with the internal ordering applications. DCS has asked the vendor to to choose another method of data transmission, but cannot force them to do so. After consulting with DCS, Group 3 determined that these were actual findings, not false positives.

**Deemed Not Reasonable**

1. **Password Configuration**

Determine if users are configured with strong passwords.  
Password parameters must meet the following complexity checks:

* 1. Require at least 8 characters
  2. Require 3 of the following:
     + Special Characters
     + Alphabetical Characters
     + Numerical Characters
     + Upper and lower case letters

Also determine the encryption type and privilege level of each user for reasonableness.

Auditor Camper reviewed the Juniper NetScreen DCS Security Report and found in section 3.5.2 and determined that the password parameters for the Primary Admin have met the complexity check and are encrypted by NetScreen.

Deemed Reasonable

## WRAP-UP

## Step 8: Observations

A. Develop observations for management letter comments and project manager. Communicate impact of audit findings on the auditors’ testwork. Document the results.

B. Obtain and document management response to management points. Document final assessment of management point to determine if point is written (in report) or verbal.

C. Include a write up of the controls in place and/or any weaknesses (findings) in a format that can be used for the next years audit planning meeting.

**Step Completed by & Date:** [Group 3 05/01/17]

**Step Reviewed by & Date:** [Insert Name & Date]

**MANAGEMENT POINTS**

Auditor developed a total of 2 potential management recommendations:

|  |  |  |
| --- | --- | --- |
| **OBS#** | **PY MP Title** | **Step #** |
| 1 | Security & Awareness Training | 5 |
| 2 | External Firewall | 6 |

Auditor communicated potential observations to: ISO Matthew Robinett on 04/12/17, 04/20/17, 04/24/17, 04/26/17

On 4/12/17, Auditor Camper emailed the ISO Matt Robinett regarding the security and awareness training policy. Auditor Camper was looking over DCS Security and Awareness training in our client response document and I would like to verify that these noted that their were somethings missing in your response they include:

General Concepts

-The concept of separation of duties

-Access controls, including creating and changing passwords and the need to keep them confidential

-Intellectual property rights, including software licensing and copyright issues

DCS responded by saying”We have recently undergone an organizational change with respect to our Information Security Analyst. We had our previous analyst move on to another organization eight months ago and was in the process of updating our IT Security Awareness and Training Program. As such, we have identified gaps in our policies and plan to update them in the following calendar year”

On 4/14/17, Auditor Camper emailed the ISO Matt Robinett regarding the external network firewall. Auditor Camper was looking over DCS's firewall for external network in our client response document and I would like to verify if DCS has a methodology for implementing patches to their firewall OS. We wanted to verify that this information isn't any other policy before we move on with the final audit work

DCS responded by saying “Our policy is to install patches when they become available. I'm not aware of a specific written statement requiring this, but we understand the need based on industry best-practices”

On 4/20/2017, Auditor Camper emailed ISO Matt Robinett about the Juniper NetScreen DCS Security Report Findings. Auditor Camper noted that the security report found two “critical” findings, and one “high” finding. Mr. Robinett was asked about the findings, and on 4/24/2017 he responded by saying that the two “critical” impact findings were part of DCS X11 service which allows machines on their network to talk to any other machine on that same network. Also Mr. Robinett noted these rules are necessary for DCS’s business purposes and don’t present a risk to the organization. After consulting with DCS, Auditor Camper noted that these two critical findings were false positives, and that it was deemed reasonable. However with the “high” finding in the security report of Telnet not using encryption, DCS responded by saying that they use Telnet because of an external vendor that requires the use of Telnet to send orders. DCS understands that Telnet sends cleartext, but cannot do business with them otherwise. DCS has stated that they have asked the vendor to choose another method of data transmission but can’t force them to do so. After consulting with DCS, Auditor Camper determined that this “high” impact finding is not a false positive and deemed it not reasonable.

Auditor officially provided DCS the observations on 5/3/2017. The Observations are embedded below:

[EMBED OBSERVATIONS]

DCS provided a response to the recommendations on 5/7/2017.

Auditor noted that DCS did concur with Group 3’s findings. On 5/7/2017, DCS management responded to the observations listed in fieldwork, via email. In this response, DCS management responded to the observations listed in fieldwork, via email. In this response, DCS concurred with the observations and provided a corrective action plan that will be distributed internally amongst relevant parties. Plans to address these concerns should occur in 2018.

Auditor determined that, based on Management’s response, 2 observations will be included in the report.

## Step 9: Final Risk Assessments

Perform final assessment of control risk. If control risk is changed then impact must be considered and documented.

**Control risk** is the risk that an error could occur in an audit area, and which could be material, individually or in combination with other errors, but the internal control system will not prevent or detect and correct the error on a timely basis.

**Step Completed by & Date:** [Group 3 & 5/10/2017]

**Step Reviewed by & Date:** [Insert Name & Date]

**FINAL RISK ASSESSMENT**

*Auditor Camper determined that the preliminary control risk is* ***high***

*The external gateway firewall is used to facilitate the exchange of data for the Consumer/Sales system and provides access for vendors, contractors, and DCS employees. This firewall is a single point of failure for the Consumer/Sales system, which provides mission essential functions, and cannot be checked for vulnerabilities. If the firewall was breached the business would be temporarily or even permanently unable to operate .*

*Security Awareness & Training is too general. There doesn’t exist proper training for niche specific jobs. Improperly trained employees leave policies and procedures up for personal interpretation which could then lead to misinterpretation and the spread of misinformation.*

## Step 10: Conclusion

Conclude to audit program objectives. All auditors completing testwork need to sign and date conclusion.

**Group sign/date:** [Group 3 and 05/10/2017]

**Project Manager sign/date:** [Matt will sign off, and Date]

**CONCLUSION**