

EDCAS Security Plan Comments

The following comments were given to Xacta for the updating of the EDCAS System Security Plan. The section titles are left as a reference.

System Name

Should state if it is a MA or GSS

ED-CAS Contacts

Should include at the very least Xacta technical support line.

Name: David Elliot

Title: Chief Information Officer (Incorrect title, should be Enterprise Architect for Information, Network Security)

Office: Information Assurance (Incorrect, should be FSA/CIO)

VDC Contacts

Should have Jim Cunningham (VDC SSO) on here as well as someone at the VDC who can be contacted if there is a problem. Vice Presidents should not be used here

Name: Matthew Baum (Should move up into section 1.3.1 since he has nothing to do with the VDC)

Title: Computer Security Officer (CSO)

Address: Room 4682-3 ROB3, 7th and D St, SW, Washington DC 20202

Phone: 202-205-0785

Email address: matthew.baum@ed.gov

Name: Keith Wilson (The person in this position is Mike Fillinich, not Keith Wilson) Update phone

Title: VDC Business Manager, FSA

Address: 830 First Street, NE, 10th Floor, Washington DC 20002

Phone: 202-377-3591 (202-377-3056)

Email: Keith.Wilson@ed.gov (Mike.Fillinich@ed.gov)

Name: Richard Jarmusik (Remove and replace with a contact at the VDC who can actually be reached in case of a problem)

Title: CSC Vice President of Operations @FSA

Address: 820 First Street, NE, First Floor, Washington DC 20002

Phone: 202-842-7390

Email: rjarmusik@csc.com

ED-CAS Security Personnel

Assignment of Security Responsibility should be made in writing and this section should provide a reference as to where that document can be found.

Name: David Elliot

Title: Chief Information Officer (Incorrect title, should be Enterprise Architect for Information, Network Security)

Office: Information Assurance (**Incorrect, should be FSA/CIO**)
Organization: Federal Student Aid (FSA), Department of Education
Address: 830 First Street, NE, 10th Floor, Washington DC 20002
Phone: 202-377-3573
Email: David.Elliot@ed.gov

VDC Security Personnel

Name: Andrew Boots (**Delete, no longer with FSA**)
Title: IT Security, FSA
Address: 830 First Street, NE, 10th Floor, Washington DC 20002
Phone: 202-377-3559
Email: Andrew.Boots@ed.gov

General Description/Purpose

The process flow is not described here. Needs to have what systems are interconnected and what information is traveling over those connections. VDC for example is the GSS that supports EDCAS. Also needs to include the types of information that EDCAS processes. Add a statement that there are no external organizations using the system.

System Environment

A bunch of unnecessary information in the first paragraph (why do we need to know there is a dining area, a lounge, a shipping and receiving area etc.) Does this effect the security of EDCAS?

Note: A more detailed description of the VDC environment is available in the Federal Student Aid (FSA) Security Plan: **Not Visual ... Virtual** Visual Data Center (VDC), June 1, 2002.

- Software
 - Windows 2000 Server with Service Pack 3(SP3).
 - Oracle Client 8.17.
 - Xacta Web C&A Application version 4.0.
 - Microsoft (MS) Office 2000.
 - Apache Webserver for Win32.
 - Standard VDC-base products that include virus protection software, Intrusion Detection System (IDS), and network monitoring devices. **Since this is a SSP for EDCAS this bullet should list what virus protection software, Intrusion Detection and network monitoring devices are being used to protect EDCAS. It shouldn't say "Standard VDC base products". Just what are these products? Verify with the VDC that these products reside as software on the hardware containing EDCAS. If this information is verified through the VDC, then reference the VDC's SSP section and page number.**

Figure 1 depicts the ED-CAS architecture previously described. **What is all the other hardware pictured at the VDC? Is it part of EDCAS or are they other systems?**

System Interconnection and Information Sharing

Should state that EDCAS is a GSS or MA and that it resides on the VDC which is a GSS.

(Are there MOU's etc. signed between EdNet and EDCAS ... if so that should be explained here.) Also what type of data is being sent back and forth between the Interconnected systems? This section should also discuss the RoB or make reference to where that information can be found ... Section 2.3 of this document (pg ?).

Applicable Laws or Regulations Affecting ED-CAS

Federal Laws and Regulations are missing from this list. This section should include not only ED information but Federal information as well. Any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system. At the very least an inclusion of FISMA and The Computer Security Act of 1987.

General Description of Information Sensitivity

This section should also describe, in general terms, the information handled by the system and the need for protective measures.

Risk Assessment and Management

It is recommended that a milestone date (month and year) be placed in this section instead of generalized terms such as "in a timely maner".

Review of Security Controls

ED-CAS has not undergone a review of its security controls by the Department of Education. The previous version of Xacta Web C&A (What version? What type of evaluation? The purpose of the review? The findings? Actions taken as a result?)

Rules of Behavior

Make the statement that users are required to sign the RoB before they can access the system.

Planning for Security in the Life Cycle

It is recommended that language describing what took place in each of the phases of the Life Cycle be discussed here. (See Appendix C of NIST Special Publication 800-18)

Authorize Processing

Make a statement about when EDCAS will go through C&A.

Personnel Security

ED-CAS has been designated as requiring its users to have a Low Risk (Level 1C) security level (This has not yet been finalized. It is recommended that people accessing EDCAS should have a minimum of a 5C due to the sensitive nature of the information stored and entered into the system).

Physical and Environmental Security

In order to cover the topics in NIST SP 800-18 for this section it is recommended that the following statement (or one similar) be included at the end of this section.

In summary, EDCAS relies on the VDC for its Physical and Environmental protection. Therefore EDCAS is covered under CSC facility policies and procedures for the following:

- The physical access control measures in place including those to restrict the entry and exit of personnel from system facility areas (see above).
- The fire safety devices in the buildings that house the system.
- The failure of supporting utilities including electric power, heating and air-conditioning systems, water, sewage, and other utilities.
- The procedures and plans to be followed in the event of a structural collapse.
- The procedures and plans to be followed in the event of a plumbing leak.
- The procedures and plans to be followed if data is intercepted.

Production and Input/Output Controls

This section should also include information about user support. The controls used to monitor the installation of, and updates to, application software should also be listed if Xacta is in any way involved in the process.

User output is not produced at the VDC but is generated by the application and (delete the word any) typically saved or printed out at the end users location.

Contingency Planning

The following information is extracted (delete for and add from) the FSA Security Plan for the VDC and applies to ED-CAS. Has EDCAS been included in the VDC DR/Contingency Plan? If yes, what are the procedures as they relate to EDCAS. A generalized statement that the VDC has DR/Contingency Plan does not cover Contingency Planning for EDCAS. This information must be verified with the VDC.

Hardware and Software Maintenance Controls

Some mention of Xacta should go in this paragraph. Again this whole section is full of vague generalized VDC procedures. This section should include specifics for EDCAS ... not just for VDC in general. Does the VDC follow all these steps of EDCAS?

This paragraph does not apply to ED. Remove it from the SSP. The Change Control Review Board (CCRB) manages change control. Clients file Customer Service Request (CSR) with one of the Service Delivery Managers (SDM). The SDM update CCRB database and the CSR are put on the agenda of the next CCRB meeting. Approved changes are documented utilizing the online CSC GIS Global Change And Request System (GCARS).

Integrity and Validation Controls

Again this whole section is full of vague generalized VDC procedures. This section should include specifics for EDCAS ... not just for VDC in general. Does the VDC follow all these steps for EDCAS? In the diagram there appears to be a CheckPoint Firewall but it doesn't look like it is protecting EDCAS so why is it mentioned here? There is no specific hardware, according to the system diagram, that is protecting EDCAS. If this is so, why is all the rest of this information in this section? The items discussed should be protecting EDCAS, not the VDC in general

Security Awareness and Training

In addition, newly assigned staff are required to attend an initial security awareness session.

Incident Response Capability

The Department of Education's Guide on Incident response has procedures to follow. That information should be included here since it is what should be followed, not CSC's procedures. CSC's procedures are secondary and can just be referenced (i.e. document name, section, page number)

Identification and Authentication

Reference the user groups in Xacta and what functions can they perform (section 4.2.1 pg.?). Describe how access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person). Describe the self-protection techniques for the user authentication mechanism (passwords are encrypted, automatically generated, are checked against a dictionary of disallowed passwords). Describe the procedures for limiting access scripts with embedded passwords.

In addition, the standard VDC policies for the systems upon which applications are hosted are provided below as extracted from the FSA Security Plan for the VDC. Does EDCAS follow this? Again this information should apply to EDCAS and not just be information about the VDC.

- Passwords must be at least 8 characters long.
- Passwords must meet at least 3 of the following criteria.
 - Uppercase letters A-Z
 - Lowercase letters a-z
 - Number(s) 0-9
 - Non-alphanumeric character (e.g.!, @, #, \$, %, etc.)
- Password may not contain your user name or any part of your full name.
- Password should not contain real dictionary words.
- Password Uniqueness set to 5.
- Lockout after 3 bad logon attempts.
- Lockout duration set to 30 minutes.
- Do not use the same user name or password on Government and CSC systems.
- Password expiration date set to 30 days.

APPENDIX A: Rules of Behavior

Add a #12 that states: I will not give my EDCAS user ID or password to anyone.

Change the last paragraph to: I agree to abide by the rules established in this document and understand that failure to comply with this agreement may result in being denied access to the system. Additional administrative action may be taken in accordance with the Department IT security policy, OCIO-1. (Delete the rest ... be grounds for administrative punishment, termination, and/or criminal prosecution.)