

## **Security and privacy questions for FSA's FY 03 Exhibit 300 response**

Lorenzo Rasetti of OMB asked FSA to revise their security responses to the FY 03 Exhibit 300 submission. Mr. Rasetti advised FSA to respond specifically to page 571 of A-11 (exhibit 300). Section F, Security and Privacy, directs FSA to address six security-related questions:

1. Are the costs of security controls understood and explicitly incorporated in the life-cycle planning of the systems, including the additional costs of meeting or exceeding the NIST standards?
2. How does the agency make sure risks are understood and continually assessed?
3. How does the agency make sure security controls are commensurate with risk and magnitude of harm?
4. What additional security controls are in place or planned for systems that promote or permit public access, other externally-accessible systems, and those that are interconnected with systems over which program officials have little or no control?
5. How does the agency use security controls and authentication tools to protect privacy for those systems that promote or permit public access?
6. How does the agency make sure that handling of personal information is consistent with relevant governmentwide and agency policies?

The following pages contain FSA's updated response. Because all these development efforts take place within the FSA development framework and system architecture blueprint, most of the text is the same for each of the six systems. For ease in review, we have italicized any special portion of the response that differs in each section.

## Section F: eCB, COD, Common School ID

The eCampus-Based (eCB) system's storage and processing happens within the FSA Virtual Data Center (VDC) and so relies on the VDC's infrastructure security controls (routers, firewalls, intrusion detection, etc.). Though eCB transactions over the Internet contain no personally-identifiable information, they are protected by the FSA standard of SSL session encryption.

The Common Origination and Disbursement (COD) system is operated principally at a commercial contractor site. This contractor handles 85% of the US personal credit card transactions every day. So the COD system inherits the security controls established to protect tens of millions of credit card numbers. Traffic between the COD site and the VDC are encrypted over a private network.

The Common School ID portion of this initiative will not result in sensitive information.

IT security for this set of systems consists of 6.3% (\$4.3 million) of contract costs. Specific security measures are described below:

1. **Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
2. **How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
3. **How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is

given to systems containing Privacy Act data or transmitting data that could result in financial disbursements.

4. **What additional controls are used for systems that have external connections?**

FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing.

5. **How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet. *The Common Origination and Disbursement system employs encryption technology as an additional secure measure to protect its Privacy Act and financial data.*

6. **How does the agency make sure it handles private information in compliance with governmentwide and agency policies?**

FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites

## **Section F: HR Modernization, VDC, FSA Portal, Security and Privacy Architecture, Datamarts, Learning Management System, Single Sign-on**

HR Modernization and LMS are operated primarily at a commercial contractor site. The systems inherit the security controls established at the commercial site.

The VDC is the central infrastructure provider for FSA. The FSA portal and the Datamarts are hosted at the VDC and rely on the VDC's infrastructure security controls.

IT Security consists of 3.6% (\$816,000) of contract costs. Specific security measures are described below:

- 1. Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
  - 2. How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
  - 3. How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is given to systems containing Privacy Act data or transmitting data that could result in financial disbursements. *Finalizing the FSA Security and Privacy architecture as part of the blueprint process, will further reduce the potential for data theft and improve protection of customer information.*
- 1. What additional controls are used for systems that have external connections?** FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems

outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing. *Because of the SLAs with the VDC, FSA policy does not require FSA systems operating within the VDC to maintain individual MOUs.*

**4. How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet. *As part of the Single Sign-On and Security and Privacy programs, FSA is developing authentication and authorization technology (including electronic signatures and encryption) to make sure only authorized users receive access to confidential information and that information comes only from trusted sources. Moreover, FSA is merging web portals for each of its business channels (Students, Schools, Financial Partners) into a single FSA portal, providing "personalized" views into user-appropriate FSA data.*

**5. How does the agency make sure it handles private information in compliance with governmentwide and agency policies?**

FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites

## Section F: CPS, FAFSA, eSign

CPS and FAFSA on the web are hosted at the VDC and rely on the VDC's infrastructure security controls.

IT Security consists of 1.9% (\$347,000) of contract costs. Specific security measures are described below:

1. **Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
2. **How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
3. **How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is given to systems containing Privacy Act data or transmitting data that could result in financial disbursements.
4. **What additional controls are used for systems that have external connections?** FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing.

5. **How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet. *The eSignature initiatives expand FSA's use of its PIN database from strictly authentication to an electronic signature capability, allowing its customers to electronically sign various loan notes, fulfilling FSA responsibilities under the Government Paperwork Elimination Act..*

6. **How does the agency make sure it handles private information in compliance with governmentwide and agency policies?** FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites

## Section F: NSLDS

NSLDS is hosted at the VDC and relies on the VDC's infrastructure security controls.

IT Security consists of 0.7% (\$127,000) of contract costs. Specific security measures are described below:

- 1. Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
- 2. How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
- 3. How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is given to systems containing Privacy Act data or transmitting data that could result in financial disbursements.
- 4. What additional controls are used for systems that have external connections?** FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing.

5. **How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet.

6. **How does the agency make sure it handles private information in compliance with governmentwide and agency policies?** FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites

## Section F: FMS, eAudit, e-Lending

FMS, eAudit, and eLending are hosted at the VDC and rely on the VDC's infrastructure security controls.

IT Security consists of 3.9% (\$655,000) of contract costs. Specific security measures are described below:

- 1. Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
- 2. How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
- 3. How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is given to systems containing Privacy Act data or transmitting data that could result in financial disbursements.
- 4. What additional controls are used for systems that have external connections?** FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing.

5. **How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet.

6. **How does the agency make sure it handles private information in compliance with governmentwide and agency policies?**

FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites

## Section F: DL e-Servicing

DL e-Servicing is hosted at the VDC and relies on the VDC's infrastructure security controls.

IT Security consists of .3% (490K) of contract costs. Specific security measures are described below:

1. **Are security costs included as part of life-cycle planning?** FSA systems follow a documented Security Lifecycle (SLC) as part of the standard system development lifecycle. The SLC provides guidance to developing and existing FSA systems to make sure security processes are followed and appropriate artifacts are produced. At the end of each lifecycle phase, the system security officer and the system manager sign a security checklist. Like all other Department of Education organizations, FSA will begin performing **annual** risk assessments, security plans updates, and certification and accreditation (C&A), exceeding NIST frequency standards. These activities add additional security costs to FSA systems. Program planners use FSA estimating guidelines to identify the approximate cost of mandated security controls.
2. **How are risks understood?** The Department of Education (and therefore FSA) require annual risk assessments and C&A. By performing these annually, FSA program managers and executives are consistently aware of the risk environment and security controls for each system. All risk assessments and C&A packages are reviewed by the Department of Education and are reviewed and signed-off by FSA senior management. In addition to independent reviews, each system is assigned a System Security Officer, who reports security issues to the system manager.
3. **How are we sure controls are commensurate with risk and possible damage?** FSA performs a sensitivity and criticality assessment on each system annually, analyzing the system's confidentiality, integrity and availability requirements. These assessments are used to make sure the security controls on each FSA system are commensurate with the risks and magnitude of possible harm, and are used to determine the amount of security investment required for each system and for supporting infrastructure (VDC, EAI, SAIG, etc.). Special security consideration is given to systems containing Privacy Act data or transmitting data that could result in financial disbursements.
4. **What additional controls are used for systems that have external connections?** FSA maintains security policies for interconnections with other systems and for systems that have public connections. For systems with connections to other systems outside of a program official's control, FSA creates Service Level Agreements and/or Memoranda of Understanding to specify respective responsibilities for security outcomes. Schools and other program participants sign agreements that spell out roles and responsibilities. For systems that permit public access, security funding is budgeted to perform periodic penetration testing.

5. **How does the agency use authentication and other controls to protect privacy?**

FSA uses authentication to fulfill its privacy promise to students and parents. Student-centered FSA systems (application/repayment) use a name/SSN/DOB/four-character PIN for authentication. Trading partners use username/password technology. FSA uses SSL to protect authentication data transmitted over the Internet. *In addition, the loan servicing system provides additional privacy protections for borrowers accessing their loan data via touch-tone phone.*

6. **How does the agency make sure it handles private information in compliance with governmentwide and agency policies?**

FSA systems protect personal information and handle the information consistent with relevant government-wide and agency policies, including:

- Employees and contractors sign a privacy act statement
- Systems are identified as systems of record as appropriate
- Systems are assessed, as part of the sensitivity assessment, to determine if personal information is maintained.
- No personal/persistent cookies on FSA websites
- Privacy notices on websites