**U.S. Department of Education**

**Office of Federal Student Aid**

**Phase I – Solicitation**

**Next Generation Financial Services Environment**

# Introduction

The U.S. Department of Education, Office of Federal Student Aid (FSA), is embarking on a new transformation known as the Next Generation Financial Services Environment (NextGen). Through this initiative, the Government seeks to implement a flexible, world-class financial solution to leverage in supporting its citizens. Initially, FSA seeks to modernize its technical and operational architecture, which will be flexible enough to expand and support other financial services. This effort will also include creating a new FSA-branded omni-channel engagement approach led by a mobile-first, mobile-complete, and mobile-continuous digital platform to support a finance lifecycle. In addition to improving the overall customer experience, the new environment will seek to improve operational flexibility, enhance cost and operational efficiency, and generate better outcomes for customers and taxpayers.

This is Phase I of a two-phase source selection in accordance with 20 U.S.C. 1018a(d) and ED Acquisition Regulation (EDAR) (48 C.F.R.) 3415.302-70(b). FSA anticipates utilizing a commercial solution(s) to meet the objectives of this initiative and requests responses from interested vendors for nine components. Vendors may provide a response for an individual, multiple, or all component(s) (as shown below), so long as responses are delineated by component. Vendors are not required to provide a response for each component to be considered. Vendors are not required to have student aid experience to participate. Components include:

* **Component A:** Enterprise-wide digital platform and related middleware
* **Component B:** Enterprise-wide contact center platform, customer relationship management (CRM), and related middleware
* **Component C:** Solution 3.0 (core processing, related middleware, and rules engine)
* **Component D:** Solution 2.0 (core processing, related middleware, and rules engine)
* **Component E:** Solution 3.0 business process operations
* **Component F:** Solution 2.0 business process operations
* **Component G:** Enterprise-wide data management platform
* **Component H:** Enterprise-wide identity and access management (IAM)
* **Component I:** Cybersecurity and data protection
* **Independent quality assurance support** will be separately solicited on a similar time frame and will be responsible for assisting FSA in monitoring vendor operations and performance. Quality assurance support vendor will be independent from vendors providing other NextGen components.

# Background on FSA

FSA’s core mission is to ensure that all eligible customers benefit from Federal financial assistance – grants, loans, work-study programs, etc. – for education beyond high school. The programs FSA administers comprise the nation’s largest source of student financial aid. Every year, over 18 million students apply for Federal aid and FSA has over 42 million customers across the student lending lifecycle. FSA’s total lending portfolio is $1.3 trillion in outstanding loans including $1.1 trillion that is directly serviced. The lending portfolio is growing at 7% per annum, driven by nearly $100 billion in annual disbursements across more than 15 million annual loan originations.

In conjunction with institutions of higher learning and third-party vendors, FSA provides lending information and services across the full Federal student aid lifecycle, including:

* Application and eligibility determination: Customers learn about their options, then apply for Federal student aid through the FAFSA;
* Disbursement: For eligible customers, FSA originates most aid through higher educational institutions to FSA customers;
* Loan processing and servicing: FSA assigns customer loans to be serviced by one of nine loan servicers across four loan technology platforms;
* Recovery: For those customers who fail to pay their loans and enter recovery, FSA contracts with a debt management vendor and Private Collection Agencies (PCAs) to engage with those customers.

Within loan processing and servicing, servicer partners perform a complete set of Federal student loan servicing activities including: customer service; loan counseling; billing and payment application and processing; repayment plan adjustments and application of benefits such as deferments, forbearance, or loan forgiveness/discharge; outreach and default aversion; quality control; and financial and other data reporting. Individual customers may have several loans on different repayment plans and may have entered special programs (e.g., Public Service Loan Forgiveness (PSLF), Total and Permanent Disability (TPD), or Teacher Education Assistance for College and Higher Education (TEACH)).

Each of the nine servicers operates its own engagement layer with proprietary branding (e.g., websites, mobile tools, contact centers), utilizes one of four servicing platforms, and maintains certain additional technical systems. The servicing platforms are customized to service Federal student loans, which include >30 permutations of repayment plans and additional unique rules related to forbearance, deferment, discharge, loan forgiveness, and recovery. A servicer will typically retain a customer account until it is paid in full, the customer defaults, or the customer receives a loan discharge. These servicing platforms must comply with all Federal security, financial management, and audit rules, regulations, and laws.

Today’s fragmented vendor landscape has created many issues, including:

* Inconsistent customer experience for FSA’s customers. Customers move through the student aid lifecycle working with multiple vendors and partners, each with different interfaces and standards;
* Limited branding opportunities for FSA. Customers often do not understand the role the Federal government, and FSA in-particular, play in their student loan journey; and
* Operational complexity and inefficiency. Each servicer has built redundant technical and operational solutions to operate within the current portfolio-aligned operating model.

Additional information about FSA can be found in Exhibit 1 and 2, below, in the attachment “01 - As-Is”, the attachment “02 – Vision”, and the 2017 Annual Report located at: <https://www2.ed.gov/about/reports/annual/2017report/fsa-report.pdf>.

Exhibit : Today’s environment across the student aid lifecycle

|  |
| --- |
|  |

Exhibit : Today’s environment for processing and servicing

|  |
| --- |
|  |

# NextGen Financial Services Environment Goals

FSA holds one of the largest consumer loan portfolios in the world and believes it should deliver for its customers on par with world-class financial services providers. To do that, FSA has established goals for the NextGen environment including:

**First**, FSA intends to provide a world-class customer experience throughout the student financial aid lifecycle to ensure:

* Easier, more seamless customer interactions with FSA through an enterprise-wide, FSA-branded omni-channel digital platform featuring a mobile-first, mobile-complete, and mobile-continuous solution (i.e., allowing for seamless channel switching) to enable customers to receive additional support through the channel most appropriate to their needs;
* Customers receive an experience informed by a holistic understanding of their needs, refined through ongoing analysis of customer data and customer feedback and continuously improved through activities like iterative user testing;
* Customers better understand the financial implications of their student debt and make more informed decisions regarding the various repayment options and protections available to Federal customers; and
* Customers receive a consistent experience under the FSA brand across all vendors supporting NextGen.

**Second**, FSA intends to improve its operational flexibility by creating an environment that can efficiently and effectively integrate new capabilities and features, continuously improve and innovate, and adjust to stay in compliance with changing Federal rules, regulations, and law.

**Third**, FSA intends to drive greater operational efficiency; reduce complexity; improve the stability, resiliency, enterprise risk management, and cybersecurity of its systems; and ensure effective and efficient use of taxpayer dollars.

**Fourth**, FSA will measure its success in part on how well NextGen improves customer outcomes and facilitates compliance with Federal consumer protection standards.

# NextGen Financial Services Environment Vision

To accomplish FSA’s goals identified in Section III, it intends to deploy a new technical and operational architecture that provides a world-class customer experience across the entire student aid lifecycle, including both enterprise-wide solutions and solutions specifically for processing and servicing. This new model will include:

Omni-channel, enterprise-wide customer engagement led by a mobile-first, mobile-complete, and mobile-continuous solution

To enable a world-class customer experience, FSA intends to procure an enterprise-wide, FSA-branded omni-channel digital platform featuring a mobile-first, mobile-complete, and mobile-continuous solution (i.e., allowing for seamless channel switching). The digital platform will be FSA’s “digital front door” for all customer journeys. To realize this vision, the digital platform will consolidate the multiple websites, mobile applications, and contact centers that currently exist across the full customer lifecycle (from application to servicing and default). This will require the digital platform to be closely integrated with technical components to be implemented specifically for NextGen as well as a wide range of other FSA systems. This layer will provide customers with a personalized experience across multiple channels with robust self-service options and seamless escalation to additional support when needed.

Common, integrated data management

FSA envisions a solution to ensure customer touchpoints feed into a common integrated data management platform which contains all information of each student throughout the lifecycle. This common, integrated data management system will allow FSA to:

* Generate customer insights through advanced analytics that improve services and reduce risk;
* Reduce error rates to lessen customer frustration and costly mistakes; and
* Lower operating expenses through efficiency gains.

Robust cybersecurity and data protection

State-of-the-art cybersecurity protection must not only be integrated into all of the components of the NextGen environment, but enterprise-wide cybersecurity must be holistically assessed and tested on an ongoing basis to ensure customer and FSA data is consistently protected.

Integration across the enterprise and potential to further scale solutions

FSA anticipates that solutions or standards implemented during this phase will need to be integrated with additional vendors or other providers from across the student aid lifecycle and may be further expanded across the enterprise in the future. Accordingly, all solutions should be implemented with both integration and future scalability in mind, ensuring third-parties can “plug in” to use common tools and feed into common interfaces.

Procure best-in-class components to reduce complexity and improve efficiency

To service loans in a more flexible, efficient, and effective environment, FSA intends to procure best-in-class technical solutions from leading financial services providers. This model will allow business process operations providers to “plug in” these solutions while providing customers with a consistent, world-class customer experience.

See Exhibit 3 for a visual representation of the NextGen vision.

Exhibit : NextGen Vision highlighting this solicitation’s focus

|  |
| --- |
|  |

Components of the Next Generation Financial Services Environment

FSA has identified the components that it believes may be necessary to realize the goals and vision for NextGen. “VII. Component-Specific Objectives and Constraints” provides objectives and constraints specific to each component FSA intends to procure. These components are listed below and presented visually in Exhibit 4.

Vendors may provide a response for an individual, multiple, or all component(s) (as shown below), so long as responses are delineated by component (see “X. Vendor Response Instructions” for more details). Components include:

* **Component A:** Enterprise-wide digital platform and related middleware
* **Component B:** Enterprise-wide contact center platform, CRM, and related middleware
* **Component C:** Solution 3.0 (core processing, related middleware, and rules engine)
* **Component D:** Solution 2.0 (core processing, related middleware, and rules engine)
* **Component E:** Solution 3.0 business process operations
* **Component F:** Solution 2.0 business process operations
* **Component G:** Enterprise-wide data management platform
* **Component H:** Enterprise-wide identity and access management (IAM)
* **Component I:** Enterprise-wide cybersecurity and data protection
* **Independent quality assurance support** will be separately solicited on a similar time frame and will be responsible for assisting FSA in monitoring vendor operations and performance. The quality assurance support vendor will be independent from vendors providing other NextGen components.

Exhibit : Components in the Next Gen Phase 1 solicitation

|  |
| --- |
|  |

Implementation approach that minimizes risk and disruption for customers while deploying world-class solutions

As described in “VII. Component-Specific Objectives and Constraints”, “Solution 2.0” (Component D) is anticipated to be FSA’s environment for all existing customers at the time of award and “Solution 3.0” (Component C) is anticipated to be tailored for new customers. As a result, Solution 3.0 (Component C) should be more flexible and able to take advantage of more modern technical architecture than Solution 2.0. FSA recognizes that it may take time to deploy Solution 3.0. FSA also recognizes that it may not be cost-effective to service some of FSA’s older loans on Solution 3.0.

Solution 2.0 (Component D) is anticipated to serve as the primary environment for FSA’s existing customers. Solution 2.0 (Component D) will need to onboard borrower accounts from existing servicers in a time frame that minimizes disruptions for customers while ensuring completion of migration is finished prior to the end of the current servicing contracts. Given that Solution 2.0 (Component D) will need to be capable of servicing all existing customers, FSA anticipates that this solution will be capable of incorporating specialty programs such as TPD, TEACH, and PSLF. Solution 2.0 will need to provide a higher quality solution than today’s existing environment and continue to add enhancement features during the migration that support the overall goals of the NextGen Vision.

It may be possible for a single environment to meet the objectives and constraints of both solutions. Once Solution 3.0 (Component C) is deployed, FSA will determine the best distribution of loans between Solution 2.0 (Component D) and Solution 3.0 (Component C).

# Target Milestones

FSA has identified target milestones in pursuit of the NextGen goals identified in “III. NextGen Financial Services Environment Goals”.

* **Milestone 1 – Achieve early customer wins**: FSA anticipates deploying capabilities across NextGen that meaningfully improve the customer experience on an accelerated timeline after award (i.e., within 6-9 months of the award date). Potential opportunities that could fall within this milestone include, but are not limited to: launching an FSA-branded omni-channel digital presentation layer enterprise-wide (Component A); launching the FSA brand on Solution 2.0 (Component D); reducing processing times and error rates for existing customers (Component D and Component F); and/or consolidating multiple FSA phone numbers to a single, enterprise-wide IVR (Component B).
* **Milestone 2 –Migrate existing customer loans to an enhanced environment:** For Solution 2.0 (Component D) and Solution 2.0 business process operations (Component F), begin enhancing Solution 2.0 (Component D) and migrating existing servicing accounts as soon as possible after award with migration complete before the end date of the current servicing contracts. Enhancements to Solution 2.0 can continue to be tested and implemented while customer migration is ongoing.
* **Milestone 3 – Launch Solution 3.0**: Launch Solution 3.0 (Component C) by a target date of late 2019 or early 2020 and begin onboarding new FSA customers. At time of launch, Solution 3.0 (Component C) would need to be integrated with a fully operational digital platform (Component A), contact center and CRM platform (Component B), enterprise-wide identity and access management (Component H), Solution 3.0 business services providers (Component E), and other relevant components and systems. Enhancements for Solution 3.0 (Component C) and related components could continue to be built, tested, and implemented after this milestone.
* **Milestone 4** – **Identify enterprise-wide standards**: Quickly identify an enterprise-wide identity and access management standard (Component H), cybersecurity standard (Component I), and common data architecture (Component G) for other vendors to incorporate into solutions, within 2 months of award.

# Overarching Constraints

Components will be subject to overarching constraints including:

* **Integration:** Solutions must include features to allow them to easily integrate with NextGen, other FSA systems, and other third-party solutions. All vendors will also be responsible for taking the steps necessary to connect their solution(s) with other components of NextGen and FSA’s existing systems where necessary to realize the goals outlined in Section III.
* **Adaptability and ongoing innovation:** Solutions should be capable of efficiently and effectively adapting to changes in the FSA operating environment (including changing Federal rules, regulations, and laws) and continuously improving and innovating.
* **Broad accessibility for customers:** Solutions must meet or exceed existing Federal rules, laws, and regulations applicable to the FSA operating environment related to solution accessibility.
* **Cybersecurity:** Solutions must include robust cybersecurity protections and features to ensure customer data is protected (illustrative technical constraints for existing security standards are included in the attached “03-Technical Constraints Compendium”).
* **Technical constraints:** Solutions must meet or exceed existing Federal rules, laws, and regulations applicable to the FSA operating environment (illustrated in the attached “03 – Technical Constraints Compendium” and “04–Attachments for Technical Constraints Compendium”) for security, program operations, payments, reporting, and websites.
* **Quality control:** Solutions must include the appropriate quality and internal controls and management oversight to ensure that best-in-class service is being provided.

Contents included in “03-Technical Constraints Compendium”:

For an illustrative view of FSA’s current environment, vendors are encouraged to refer to the attached compendium of constraints (“03 – Technical Constraints Compendium”) and attachments referenced (“04–Attachments for Technical Constraints Compendium”). Most of these constraints are derived from existing laws, regulations, and Federal agency guidance (e.g., NIST security requirements, FedRAMP requirements). These constraints frequently change due to acts of Congress and updates to Federal regulatory and non-regulatory guidance. Constraints fall into four categories: security, payments, reporting, and websites. While NextGen vendors will be responsible for ensuring their solutions comply with existing laws, regulations, rules, and Federal agency guidance, FSA welcomes suggestions for how FSA and its vendors could better operate within the current regulatory environment.

# Component-Specific Objectives and Constraints

This section includes component-specific objectives and constraints for the components of NextGen.

**Component A:** Enterprise-wide digital platform (mobile, web, and related middleware)

*Objectives:*

The enterprise-wide digital platform provider will deliver an enterprise-wide digital solution that will serve as FSA’s digital “front door.” The platform will be world-class in design and ease of use to enable FSA’s customers to elect the digital platform as their primary channel for common customer journeys. The platform will provide a true omni-channel digital experience, including the ability to use a mobile device for all their needs (i.e. a mobile-first, mobile-complete, and mobile-continuous experience). The content and capabilities presented to customers must be grounded in FSA customer needs and guide customers in making more informed decisions. Unlike the current environment where customers navigate multiple websites and mobile applications maintained by FSA and its vendors at different points of customer journeys, customers will primarily interact with FSA through this enterprise-wide digital platform that allows for a consistent customer experience, robust self-service options, and seamless customer connection to other FSA resources (e.g., contact centers) when needed.

*Operating and solution constraints:*

* Solution must include a mobile-first, mobile-complete, mobile-continuous, omnichannel digital platform with features comparable to those deployed by leading financial services providers and other customer-centric organizations.
* Solution must ensure FSA’s current and potential future customers can easily access and understand its products and services through public content and access private content unique to each user. The digital platform will be FSA’s primary digital presence with a scope of responsibilities that includes the content and services currently provided by sites including: StudentAid.ed.gov, StudentLoans.gov, MyEdDebt.gov, NSLDS.gov, FAFSA.gov, and third-party loan servicer websites.[[1]](#footnote-2)
* To the maximum extent possible, solution must allow customers to be able to complete all customer journeys through the digital platform (e.g., submit FAFSA, check loan balance, make a payment, enroll in a payment plan). Where FSA has a viable solution already available or in development (e.g., myMoney mobile application), the digital platform will need to be able to integrate some or all of the solution(s) and/or provide a portal to that solution(s).
* Solution must include a content management system that can be easily updated and allow FSA to make direct changes to content quickly without significant reprogramming.
* Solution must encourage customers to utilize self-service solutions by making digital self-service efficient and effective across all journeys.
* Solution must allow customers to seamlessly switch channels if they need additional support.
* Solution must integrate with other components as needed regardless of the provider and have the ability to update and change quickly with minimal cost.

**Component B:** Enterprise-wide contact center, CRM, and related middleware

*Objective:*

FSA intends to provide customer support capabilities on par with world-class customer service organizations. When the digital platform (Component A) is insufficient to meet customer needs, customers will be able to contact FSA through their preferred channel (e.g., chat, social media, telephony, email). Once a customer initiates contact, that individual will receive a world-class experience that includes being quickly routed to the best available resource for their inquiry (e.g., live or AI agent) and receiving accurate and consistent information to address their need. Data gathered through direct customer engagement should be leveraged to personalize the customer experience across channels and identify opportunities to improve the self-service digital experience.

To implement a seamless customer experience, Component B will include the following sub-components:

* **CRM:** The CRM solution will allow all customer-facing staff and vendors across the FSA environment to access a single, unified view of the customer. The CRM solution will also interface with the enterprise-wide digital platform (Component A) to ensure that customers experience a digital environment that tailors content to their needs.
* **Contact center technical backbone:** The contact center technical backbone will support multiple channels for customer communication while ensuring there is only one solution per channel (e.g. a single FSA chat platform, a single FSA phone number). The solution will effectively and efficiently utilize multiple solutions to address customer concerns (e.g. containing calls within the IVR). Where customer inquiries cannot be addressed through automated solutions or self-service, the technical backbone will route customers to the appropriate resource for live support.
* **Quality control and knowledge management:** The solution will include development of standard work products for contact center resources in the servicing environment (e.g., contact scripts, training materials) to ensure customers receive consistent and accurate support for servicing inquiries. The solution will include conducting regular quality control monitoring of customer engagement conducted by Solution 2.0 business process operations (Component F) and Solution 3.0 business process operations (Component E) resources to ensure consistent high-quality customer service across all channels. This capability will allow FSA the option to partner with multiple vendors to provide call center capabilities while ensuring consistency across those vendors.

*Additional operating and solution constraints:*

* CRM:
  + Deploy a proven customer relationship management (CRM) solution for Solution 3.0 (Component C) and Solution 2.0 (Component D) that has the capability to interface with multiple data sources and channels across the FSA enterprise.
  + Allow authorized staff and partners to access and extract certain data and reports, including a function that allows authorized higher education officials to access relevant student data as permissible under existing laws and regulations.
  + CRM will also serve as the agent desktop solution for the servicing-related contact centers provided by the Solution 3.0 business process operations (Component E) and Solution 2.0 business process operations (Component F).
* Contact center technical backbone:
  + Transfer customers with inquiries that do not pertain to servicing to the appropriate contact centers (e.g. Student Loan Support Center, FSAIC, FSA ID Call Center, Loan Consolidation Call Center, Default Resolution Group, Ombudsman, and Enterprise Complaint System) while demonstrating the ability to ultimately address all these customer inquiries within the solution.
  + Transfer servicing-related contacts to either a Solution 3.0 business process operations vendor (Component E) or a Solution 2.0 business process operations vendor (Component F) depending on where the customer’s loan sits.
  + Evaluate drivers of customer demand and deploy capabilities that reduce the need for live agent support.
* If multiple tools are necessary to support all channels, ensure that those tools are integrated to maintain a single customer view across all channels.
* Solution must integrate with other components as needed regardless of the provider and have the ability to update and change quickly at minimal cost.

**Component C:** Solution 3.0 (core processing, related middleware, and rules engine)

*Objective:*

Solution 3.0 should serve as the environment for FSA’s new customers and will provide the technical systems necessary to service loans for customers with the loans and repayment plans that FSA offers today. It will also be highly adaptable to support future products and services FSA may provide. This solution will identify cost efficiencies through increased automation and greater flexibility (e.g., through innovative middleware and/or microservices solutions), relying on streamlined manual processing operations (Component E) if automation is not feasible. Solution 3.0 will have significantly greater flexibility than Solution 2.0 (Component D) to support changing servicing rules, laws, and regulations and the ability to quickly implement new functionality with minimal operational complexity. Relative to the current FSA environment, Solution 3.0 will ensure more consistent application of servicing rules, prove more adaptable to a shifting regulatory environment, and provide a more flexible, technology-enabled system that reduces error rates and processing expense.

*Operating and solution constraints:*

* Perform all loan servicing functions for the currently available loans and repayment plans in the Federal student loan environment, including:
  + Loan servicing functions that include, among others, calculating payments due, payment application, balance calculations including capitalized interest, and loan status tracking;
  + Support for retroactive processing, including the retroactive application of deferments, forbearances, payments, and other transactions;
  + Processing traditional repayment plans including Standard, Graduated, and Extended, as well as combinations thereof;
  + Processing income-driven repayment plans including Income-Contingent, Income-Based, Pay-As-You-Earn, and Revised-Pay-As-You-Earn;
  + Supporting income-driven plans’ specific eligibility requirements; allowing for variable payments that are tied to a customer’s income, family situation, and other characteristics which may fluctuate; and require annual recertification and recalculation;
  + Supporting switching across repayment plans; and
  + Scaling to anticipated volumes of loans serviced.
* Provide loan servicing functions for various customer classes and loan statuses, as well as special programs, within the Federal student loan environment of today, including, but not limited to: Loans to customers in school and in the grace period; TEACH grants; military customers; PSLF and other loan forgiveness programs; TPD and other loan discharge programs; loans in forbearance, deferment, and various stages of delinquency; and loan consolidation.
* Provide the ability to maintain a robust data history, including retroactive processing (e.g., “as-was” vs “as-is”), and tracing loans through consolidation transactions.
* Provide the ability to easily scale as volumes increase and quickly implement new processing functionalities with minimal major technical interventions.
* Allow third-party providers to engage with (“plug into”) the system to complete processes necessary to effectively serve customers as outlined under component specific-objectives and constraints for Solution 3.0 business process services (Component E).
* Solution must integrate with other components as needed regardless of the provider and have the ability to update and change quickly at minimal cost.

**Component D:** Solution 2.0 (core processing, related middleware, and rules engine)

*Objective:*

Solution 2.0 should serve as the environment for FSA’s existing customers, with capabilities enhanced beyond those present in today’s loan servicing environment. Solution 2.0 will initially provide the full suite of technical capabilities associated with servicing loans in the FSA environment, from front-end customer engagement down to the technical solution supporting the processing and servicing of loans, with enhancements provided where possible to improve customer experience and operational flexibility. Solution 2.0 will migrate loans from existing platforms on an accelerated time frame following the contract award and provide all technical solutions necessary to service a loan. Where resources are needed for operational functions, Solution 2.0 will provide mechanisms for the Solution 2.0 business process operations solution (Component F) to operate within the Solution 2.0 system boundaries. Solution 2.0 will deploy advanced capabilities to provide customers with a world-class experience, improve automation and system flexibility, and reduce operational complexity and inefficiency for FSA. Solution 2.0 will ultimately phase out certain customer engagement capabilities when it integrates with the proposed, enterprise-wide digital platform (Component A), enterprise-wide contact center platform (Component B), and enterprise-wide identity and access management solution (Component H).

*Operating and solution constraints:*

* Solution 2.0 (Component D) must address the constraints identified for Solution 3.0 (Component C). In addition, Solution 2.0 (Component D) must address the following constraints:
  + Provide world-class service, enhanced beyond today’s environment, while continuing to meet the requirements currently placed upon Title IV Additional Servicers for all loans and repayment plans currently in FSA’s portfolio;
  + Onboard student loans from existing servicers quickly after award on a schedule that maximizes FSA operational and cost efficiency while minimizing borrower disruption (see “01 - As-is” attachment for further details on loan breakdown across existing providers and across loan types);
  + Demonstrate the capability to effectively and efficiently transfer loans to Solution 3.0 (Component C); and
  + Provide transitional engagement layer solutions for existing customers while the enterprise-wide digital platform (Component A), contact center platform (Components B), and enterprise-wide identity and access management solution (Component H) are implemented. Solution will successfully integrate with these components once they are operational and phase out redundant capabilities.

**Component E:** Solution 3.0 business process operations

*Objective:*

The Solution 3.0 business process operations solution(s) will support the efficient and effective operation of the NextGen environment under FSA’s brand by providing the business process resources necessary to initiate engagement with FSA’s customers, respond to inbound customer contacts, and perform servicing functions that cannot be automated. Solution(s) will drive world-class customer experience by identifying strategies to improve self-service functionality and efficiently and effectively process back-office needs for FSA customers. These resources will provide an enhanced level of service than today’s environment and one that is consistent with leading financial services providers and other industry-leaders recognized for their customer service.

Component E includes the following sub-objectives:

* **Customer engagement and outreach:** The solution will develop and execute outbound engagement campaigns to achieve FSA’s goals, based on a deep understanding of customer needs.
* **Contact center support:** The solution will be equipped to provide world-class customer experience in responding and resolving inbound customer inquiries across multiple channels.
* **Loan processing:** The solution will efficiently complete back-office activities related to loan servicing that cannot be automated while interfacing with other relevant components. Solution will seek to identify additional processes that can be streamlined or automated to achieve additional cost efficiencies and minimize errors.

*Operating and solution constraints:*

* Customer engagement and outreach
  + For customers whose loans sit on Solution 3.0 (Component C), this vendor(s) will print and mail all servicing-related materials.
  + For all customers, this vendor(s) will process inbound servicing-related physical mail and route it to the appropriate destination for both Solution 3.0 (Component C) and Solution 2.0 (Component D).
* Contact center support
  + Perform contact center operations for customers with loans on Solution 3.0 (Component C) while operating within the system boundaries of the agent desktop/CRM solution provided by the enterprise-wide contact center (Component B).
* Loan processing
  + Provide processing capabilities as required by Solution 3.0 (Component C) including the review, validation, and processing associated with enrollment, applications, and requests for various borrower programs and loan status adjustment, such as:
    - Income-driven repayment plan processing, including application and eligibility review, income checks and payment calculations, and annual recertification activities;
    - Processing associated with military service members, including requests for deferment and forbearance, SCRA benefits, and hostile pay benefits;
    - School and customer enrollment processing, including manual entry of hard-copy applications;
    - Deferment and forbearance application processing;
    - Loan consolidation request processing;
    - Special programs processing, including applications and transfers associated with TPD and loan forgiveness programs; and
    - Processing related to specialty claims, including death, closed school, and borrower defense requests.
  + Conduct error and dispute resolution investigation and processing, including:
    - Direct and indirect credit bureau disputes filed by customers or initiated by the credit bureaus;
    - Account maintenance, including manual correction of errors identified through data integrity scans and in response to FSA change requests; and
    - Payment processing, including researching lost or misapplied payments and payment reapplication at the request of customers or FSA.
  + Operate within the system boundaries of the technical solutions provided by Solution 3.0 (Component C) and enterprise-wide contact center solution (Component B).

**Component F:** Solution 2.0 business process operations

*Objective:*

The Solution 2.0 business process operations provider(s) will support the efficient and effective operation of the NextGen environment under FSA’s brand by providing the business process resources necessary to initiate engagement with FSA’s customers, respond to inbound customer contacts, and perform servicing functions that cannot be automated. Provider(s) will drive world-class customer experience by identifying strategies to improve self-service functionality and efficiently and effectively process back-office needs for FSA customers. These resources will provide an enhanced level of service than today’s environment and one that is consistent with world-class financial services providers and other industry-leaders recognized for their customer service. This component will enable a seamless transition from utilizing transitional engagement layer technologies for Solution 2.0 (Component D) to the enterprise-wide engagement layer (Component A & B) once implemented for FSA’s existing customers.

Component F includes the following sub-objectives:

* **Customer engagement and outreach:** The solution will develop and execute proactive outbound engagement campaigns to achieve FSA’s goals, based on a deep understanding of customer needs, for Solution 2.0 (Component D) loan customers.
* **Contact center support:** The solution will be equipped to provide world-class customer experience in responding and resolving inbound customer inquiries across multiple channels for Solution 2.0 (Component D) loan customers, utilizing Solution 2.0’s transitional engagement layer (Component D) and the enterprise-wide engagement layer once implemented (Component A & B).
* **Loan processing:** The solution will efficiently complete back-office activities related to Solution 2.0 (Component D) loan customers that cannot be automated. Solution will seek to identify additional processes that can be streamlined or automated to achieve additional cost efficiencies and minimize errors.

*Operating and solution constraints:*

* The Solution 2.0 business process operations solution(s) (Component F) must meet all constraints associated with “Loan processing” for Solution 3.0 business process operations (Component E) (but not those constraints related to “Customer engagement” or “Contact center support” for Component E) with the following additions:
  + While the enterprise-wide digital engagement layer is being implemented (Component A and Component B), perform all contact center activities and back-end processing functions that cannot be automated within Solution 2.0 (Component D) system boundaries;
  + Once the enterprise-wide digital engagement layer (Component A & Component B) is implemented, perform all contact center activities for customers whose loans sit on Solution 2.0 (Component D) within the operating system boundaries of the agent desktop/CRM solution provided by the enterprise-wide contact center solution (Component B); and
  + For customers whose loans sit on Solution 2.0 (Component D), print and mail all servicing-related materials. Solution will need to process inbound servicing-related physical mail while Solution 3.0 business process operations (Component E) is implemented.

**Component G:** Enterprise-wide data management platform

*Objective:*

The enterprise-wide data management platform will support accurate record-keeping and data analytics across the FSA enterprise. It will seamlessly integrate data sources and create a common data architecture to eliminate the fragmentation and inconsistency of data in today’s environment.

*Operating and solution constraints:*

* Determine a master data management and governance (MDM) architecture that allows for a master record of a customer’s loan history, interfacing with relevant FSA systems including, Solution 2.0 (Component D) and Solution 3.0 (Component C), and other relevant data sources to support accurate record-keeping, system operations, and enhanced data analytics. The MDM architecture should have the potential to serve as the standard data architecture solution and to be scaled across the entire FSA enterprise.
* Provide a single view of all customers across the enterprise that enables analytics and reports to be run on customer data.
* Provide advanced analytical tools and capabilities (e.g. data preparation, visualization) necessary to derive meaningful, real-time insights into customer behavior. Make these tools and capabilities available for use by FSA and authorized FSA contractors.
* Support FSA by providing data analytics support including, but not limited to, dedicated support from specialists (e.g., data scientists, data engineers) who can generate data insights that informs FSA’s strategic objectives and specific decisions regarding customer engagement.

**Component H:** Enterprise-wide identity and access management

*Objective:*

Deploy a world-class identity and access management solution that easily integrates with other solutions and serves all FSA users (customers, staff, contractors, guaranty agencies and lenders, postsecondary education officials, and other authorized third parties).

*Operating and solution constraints:*

* Allow for single sign on across all FSA systems, including customer verification within the environment that is user-friendly while supporting critical security capabilities. Systems in-scope include, but are not limited to: all NextGen components included in this solicitation and FSAID, COD, NSLDS, FMS, and PEPS.
* Meet NIST Special Publication 800-63-3, Digital Identity Guidelines for information on the level of assurance at Identity Assurance Level (IAL) 3, Authenticator Assurance Level (AAL) 3, and Federation Assurance Level (FAL) 3.
* Solution will need to be able to migrate all users to an authentication solution with minimal disruption
* Enterprise-wide identity and access management provider must be able to meet existing (or similar) FSA operating environment constraints referenced in “VI. Overarching Constraints”, including those related to security, payment, reporting, and other applicable constraints.

**Component I:** Enterprise-widecybersecurity and data protection solutions

*Objective:*

Cybersecurity and data protection solutions will provide FSA the ability to protect its data and systems and monitor, manage, and remediate cyberattacks and information security risks across the enterprise.

*Operating and solution constraints:*

* As specified in “VI. Overarching Constraints,” solutions must include robust cybersecurity protections and features to ensure customer data is protected that meet existing Federal rules, laws, and regulations applicable to the FSA operating environment (illustrative technical constraints for existing security standards are included in the attached 03-Technical Constraints Compendium).

# Expected Volumes

FSA expects that when NextGen is implemented, many of the customer engagement figures will significantly change (e.g., digital platform with greater self-service functionality will create less need for inbound calls and outbound postal mailings). Expected volumes relevant to the NextGen environment include:

* Size of business
  + >37 million customers being serviced in the FSA environment (with an additional 5 million serviced through the FFEL program outside of the FSA environment)
  + Lending portfolio that exceeds $1 trillion in outstanding principal
  + Over 18 million loans were assigned to servicers last year with a significant proportion (58%) assigned between August and October
  + Customer base projected to grow over 40% between 2017-26
* Customer engagement for servicing
  + The current servicing environment supports a high volume of inbound and outbound customer engagement.
  + Inbound communications
    - Over 15 million online accounts accessed each month
    - Over 2 million inbound calls per month with an average handle time of ~7 minutes
    - ~500,000 incoming mails per month
    - Over 180,000 incoming emails per month
    - ~45,000 customer complaints per month
  + Outbound communications
    - Over 35 million outbound emails per month
    - Over 30 million outbound calls initiated per month
    - Over 7 million pieces of outbound mail per month
* Loan payments processed
  + Over 200 million payment transactions are processed per year
* Loan processing
  + Over 450,000 customers submit annual re-certifications for an income-driven repayment plan each month
  + Over 300,000 loans are closed or discharged each month due to death, disability, are paid in full, or for other reasons (not including consolidation)
  + Over 250,000 customers change their repayment plan each month, impacting the status of ~1.3 million loans
  + On average, over 350,000 loans are transferred from servicing to FSA’s Debt Management and Collection System (DMCS) each month
  + ~75,000 customers submit certification for TEACH grants each month
  + ~70,000 customers consolidate their loans each month impacting an average of five loans per borrower
  + ~35,000 customers submit certification for PSLF each month
  + Over 10,000 customers submit certifications for TPD each month

# Selection factors

This is Phase I of a two-phase source selection in accordance with 20 U.S.C. 1018a(d) and ED Acquisition Regulation (EDAR) (48 C.F.R.) 3415.302-70(b). The Government will review each response component by component. The following are the factors on which vendors submitting responses will be selected for consideration for Phase II of this selection process:

Selection Factor 1

*Strategic Fit* – Responses will be reviewed to assess the degree to which the solution included in the vendor’s response enhances FSA achievement of its goals while likewise minimizing risk and meeting scheduled milestones. These goals include, but are not limited to:

* Delivery of a world-class customer experience
* Achievement of greater operational flexibility
* Reduction in complexity
* Improvement in customer outcomes of FSA programs

Selection Factor 2

*Past Performance* – Responses will be reviewed to assess how the vendor’s past performance experience indicates success in deploying world-class solution(s) of similar complexity and scope for the component(s) vendor is submitting a response for. Past performance examples should include a broad range of relevant experience and are not limited to experience with student aid. Responses will also be reviewed to determine the quality of past performance in respect to timeliness, quality, and cost management.

Selection Factor 3

*Cost/Price* – Responses will be reviewed to assess whether cost submitted:

* Is a cost likely to be associated with the solution offered;
* Delivers to the Government price(s) consistent with those offered to the offeror’s best, most favored customers; and
* Demonstrates innovation in managing and reducing cost over the span of the contract and passing all or a portion of savings to your customer(s).

Selection Factor 4

*Understanding of the student aid financial services environment* - For vendors submitting responses for Components C, D, E, and F, responses will be assessed to determine if the offeror’s response demonstrates an understanding of the current student aid financial services environment. Vendors do not need previous experience with Federal student aid to demonstrate this understanding.

Selection for Participating in Phase II

Responses will be reviewed under Selection Factors 1, 2, 3, and 4 (for applicable components). Selection Factor 1 is significantly more important than Selection Factors 2, 3, and 4.

In accordance with EDAR 3415.302-70(b)(3), the Contracting Officer will select the vendors that are eligible to participate in Phase II of this procurement. This selection will be based on the Contracting Officer’s determination of which vendor(s) submit the most advantageous component solution(s) to the Government.

The Contracting Officer will limit the number of selected vendors to the number of sources that the Contracting Officer determines is appropriate and in the best interests of the Government. Only sources selected in Phase I will be eligible to participate in Phase II.

# Vendor Response Instructions

Vendors may provide a response for an individual, multiple, or all component(s). In accordance with EDAR 3415.302-70(b)(2), each vendor shall submit a written response, to include the following:

Executive Summary

A high-level overview of the vendor, vendor contact information, identification of which component(s) vendor is providing a response for, and information about the vendor that it feels is important to showcasing their capabilities.

Solution

For each component(s) to which the vendor wishes to respond, (as well as for a combined solution if the response includes multiple components), vendor shall submit a narrative describing how the NextGen Financial Services Environment goals will be met, taking into account the overarching constraints, milestones, and component-specific objectives and constraints detailed in this solicitation.

Past Performance

Vendor shall submit up to 3 past performance references. References shall collectively provide past performance for each component addressed in the response. References shall include contact name, phone number, and email. Past performance references shall include a broad range of relevant experience and should not be limited to experience with student aid. Past performance references shall be consistent with the vendor’s projects/programs, completed within the last 5 years. Vendor shall highlight previous experience in delivering and/or developing successful solutions to enable world-class delivery of financial services. This includes details on how vendor previously defined objectives and implementation plans, met cost objectives (including, but not limited to, implementation and build costs), met benefit objectives, implemented and overcame functional and organizational challenges, mitigated risks, and ultimately delivered successful solutions with measurable business outcomes (e.g., improved customer satisfaction, lowered operating costs, increased digital interactions) in financial services environments. Response shall also include deployment environment and development timeline and cost.

Cost/Price

For each component(s) to which the vendor is responding, submit the costs likely to be associated with the approach, including:

* Individual component cost (using the attached template, “06 – Price Cost Template” where relevant), including:
  + Cost to FSA to implement/build component solution, if any. Ranges are permitted. Include pricing methodology in a supplemental narrative attached to the template.
  + The best price currently available to a commercial customer for implementation/build and rationale for any differences between the best price currently available to a commercial customer and the Government
  + Ongoing operational costs to FSA for component solution, if required. Ranges are permitted. Include pricing methodology in a supplemental narrative attached to the template.
  + The best price currently available to a commercial customer for ongoing operational costs, if required, and rationale for any differences between the best price currently available to a commercial customer and the Government.
  + Migration/cost support which would be made available to a commercial customer for a like endeavor, if any, and how similar support might apply to NextGen. Include this information in a supplemental narrative attached to the template.
* In addition to the information included in the template and supplemental narratives for individual component cost, vendor shall submit an overall implementation/build cost for all components addressed in the response in a supplemental narrative. Ranges are permitted. Include pricing methodology.
* In addition to the information included in the template for individual component cost, vendor shall submit an overall operational cost for all components addressed in the response in a supplemental narrative. Ranges are permitted. Include methodology.

Response shall also include an explanation of potential savings to the Government resulting from your approach. This may include details on how to share potential future cost savings that may result from technology or business process improvements or economies of scale. In addition, responses should include up to five examples of methods currently utilized in commercial practice to drive superior performance in each component (e.g. Service Level Agreements, Service Level Standards, incentives, disincentives, etc.).

Student Aid Financial Services Environment

For Components C, D, E, and F, submit a narrative describing vendor’s understanding of the current student aid financial services environment.

Teaming Arrangements/Subcontracting

Vendor shall include in its response a listing of any team member(s) or potential sub-contractor(s), including their respective role and responsibilities using the attached template “07-Teaming Arrangements and Subcontracting Template.”

# Additional Information

Two-Phase Solicitation Process

Only those vendors selected in Phase I will be provided the Phase II solicitation(s) and/or permitted to submit an offer in Phase II. No contract will be created as a result of the Phase I solicitation and the Government will not reimburse any vendor’s response preparation cost. Selection in Phase I of this solicitation does not constitute, nor guarantee, a contract award.

Teaming Arrangements/Subcontracting

The Government anticipates that teaming arrangements may be entered into. However, no exclusive teaming arrangements may be made. The Government intends to exercise broad authority in interacting with key subcontractors.

Small Business Utilization

The Government expects the selected vendor(s) to meet the Government’s small business subcontracting goals to the maximum extent practicable. The small business subcontracting goals for FSA can be found at <https://www2.ed.gov/policy/fund/reg/clibrary/sbgoals.html>.

Response Submission Methods

Responses shall be submitted using electronic mail (email) only. Responses shall be sent to [MPDSETeam@ed.gov](mailto:MPDSETeam@ed.gov). All responses shall be included as attachments formatted using PDF Format with a duplicate copy compatible with Microsoft Word 2010, Microsoft PowerPoint 2010, and/or Microsoft Excel 2010.

The subject line of the email shall read “Phase I Submission – NextGen Financial Services Environment.”

Page Limitations

Page limitations are included for each section in the below table. The response shall be accompanied by a cover letter prepared on the company’s letterhead stationery. The cover letter shall identify all enclosures being transmitted and shall be used only to transmit the response and shall include no other information.

Vendor responses may include pages larger than 8 ½” x 11”; however, such pages will count as two or more pages, rounding up to the next increment of 8 ½” x 11”. Font sizes for text portions of the strategic fit and past performance shall not be smaller than Times New Roman, 12 point or approximate equivalent. The font size restriction does not apply to text in charts or similar presentations. Margins should be kept at 1” on all four sides of the page. Footer of submission should include page numbers.

In the event that the page limitation stated herein is exceeded, the Government reserves the right to review only the pages of the submission within the below constraints, or what the Government deems to be the equivalent of the first number of pages up to the page limit.

| **Volume** | **Page Limit** |
| --- | --- |
| I. Executive Summary | *2* |
| II. Solution (Overall) | *7* |
| IIa. Solution (Component A: Enterprise-wide digital platform) | *5* |
| IIb. Solution (Component B: Enterprise-wide contact center platform, CRM, and related middleware) | *5* |
| IIc. Solution (Component C: Solution 3.0) | *10* |
| IId. Solution (Component D: Solution 2.0) | *10* |
| IIe. Solution (Component E: Solution 3.0 business process operations) | *5* |
| IIf. Solution (Component F: Solution 2.0 business process operations) | *5* |
| IIg. Solution (Component G: Enterprise-wide data management platform) | *5* |
| IIh. Solution (Component H: Enterprise-wide identity and access management (IAM)) | *5* |
| IIi. Solution (Component I: Cybersecurity and data protection) | *5* |
| III. Past Performance | *10* |
| IV. Cost/Price | *No limit, use table “06-Price Cost Template” as part of response* |
| V. Student Aid Financial Services Environment (for Components C, D, E, and F) | *5* |
| VI. Teaming Arrangements/Subcontracting | *Use table “07-Teaming Arrangements and Subcontracting Template”* |

Submission Deadline

All questions regarding this solicitation shall be submitted to [MPDSETeam@ed.gov](mailto:MPDSETeam@ed.gov) and received by the Government no later than 3:00PM Eastern on February 26, 2018.

Use the attached table (“08-Question Template”) for submitting questions.

Responses shall be submitted and received by the Government no later than 3:00PM Eastern on April 6, 2018. The time of receipt is considered to be the time in which the email is received at the initial point of entry to the Department infrastructure. Delays in transmission or other electronic issues experienced will not extend the due date or time; thus, vendors are encouraged to submit all responses well in advance of the due date and time.

Terms and Conditions

FSA anticipates including, at a minimum, the following terms and conditions in the Phase II solicitation(s). The content required in these clauses may be required in Phase II but not as part of Phase I.

**Federal Acquisition Regulations** (Full text of these clauses can be found at <https://www.acquisition.gov/browsefar>):

52.204-19 Incorporation by Reference of Representations and Certifications (Dec 2014)

52.233-4 Applicable Law For Breach Of Contract Claim (Oct 2004)

52.212-4 Contract Terms and Conditions -- Commercial Items (Jan 2017)

52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Nov 2017)

*The Contracting Officer will indicate which clauses in 52.212-5 will be included in the Phase II solicitation(s).*

52.239-70 Access to Contractor and Subcontractor Information Systems and Related Resources in Carrying Out Privacy and Information Security Inspections (Deviation) (Aug 2016)

**Department of Education Acquisition Regulations**

*For Phase I, please use the “Legacy” information at the website listed in paragraph (a) of 3452.239-71 and 3452.239-72.*

**3452.239-71 Notice to Offerors of Department Security Requirements (MAR 2011)**

(a) The offeror and any of its future subcontractors will have to comply with Department security policy requirements as set forth in the “Bidder's Security Package: Security Requirements for Contractors Doing Business with the Department of Education” at: *http://www.ed.gov/fund/contract/about/bsp.html.*

(b) All contractor employees must undergo personnel security screening if they will be employed for 30 days or more, in accordance with Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings,” available at: *http://www.ed.gov/fund/contract/about/acs/acsom5101.doc.*

(c) The offeror shall indicate the following employee positions it anticipates to employ in performance of this contract and their proposed risk levels based on the guidance provided in Appendix I of Departmental Directive OM:5–101:

High Risk (HR): [Specify HR positions.].

Moderate Risk (MR): [Specify MR positions.].

Low Risk (LR): [Specify LR positions.].

(d) In the event the Department disagrees with a proposed risk level assignment, the issue shall be subject to negotiation. However, if no agreement is reached, the Department's risk level assignment shall be used. The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data to be accessed, and the type of information technology (IT) system access required. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause.

(End of Provision)

**3452.239-72 Department Security Requirements (MAR 2011)**

(a) The contractor and its subcontractors shall comply with Department security policy requirements as set forth in the “Bidder's Security Package: Security Requirements for Contractors Doing Business with the Department of Education” at *http://www.ed.gov/fund/contract/about/bsp.html.*

(b) The following are the contractor employee positions required under this contract and their designated risk levels:

High Risk (HR): [Specify HR positions.]

Moderate Risk (MR): [Specify MR positions.]

Low Risk (LR): [Specify LR positions.]

(c) All contractor employees must undergo personnel security screening if they will be employed for 30 days or more, in accordance with Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings.” The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data to be accessed, and the type of information technology (IT) system access required. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause.

(d) The contractor shall—

(1) Ensure that all non-U.S. citizen contractor employees are lawful permanent residents of the United States or have appropriate work authorization documents as required by the Department of Homeland Security, Bureau of Immigration and Appeals, to work in the United States.

(2) Ensure that no employees are assigned to high risk designated positions prior to a completed preliminary screening.

(3) Submit all required personnel security forms to the contracting officer's representative (COR) within 24 hours of an assignment to a Department contract and ensure that the forms are complete.

(4) Ensure that no contractor employee is placed in a higher risk position than that for which he or she was previously approved, without the approval of the contracting officer or the COR, the Department personnel security officer, and the Department computer security officer.

(5) Ensure that all contractor employees occupying high-risk designated positions submit forms for reinvestigation every five years for the duration of the contract or if there is a break in service to a Department contract of 365 days or more.

(6) Report to the COR all instances of individuals seeking to obtain unauthorized access to any departmental IT system, or sensitive but unclassified and/or Privacy Act protected information.

(7) Report to the COR any information that raises an issue as to whether a contractor employee's eligibility for continued employment or access to Department IT systems, or sensitive but unclassified and/or Privacy Act protected information, promotes the efficiency of the service or violates the public trust.

(8) Withdraw from consideration under the contract any employee receiving an unfavorable adjudication determination.

(9) Officially notify each contractor employee if he or she will no longer work on a Department contract.

(10) Abide by the requirements in Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings.”

(e) Further information including definitions of terms used in this clause and a list of required investigative forms for each risk designation are contained in Departmental Directive OM:5–101, “Contractor Employee Personnel Security Screenings” available at the Web site listed in the first paragraph of this clause.

(f) Failure to comply with the contractor personnel security requirements may result in a termination of the contract for default.

(End of Clause)

**Federal Student Aid Local Clauses**

**FSA 37-2 Alternate 1 Continuation of Mission Critical Contractor Services (OCT 2012)**

(a*)* Definition*.* As used in this clause*—*

(1) Mission Critical Contractor System or Other Services are defined as a system or other services residing at the Data Center that have a material impact on the accomplishment of the Federal Student Aid mission.

(b) The services under this contract are vital to the mission of the Department of Education (ED). The Contractor shall be responsible for the availability of all systems operated at the Data Center pursuant to this contract, or other services performed by the Contractor for ED. This clause applies to all or any part of the contract that includes services that directly support the agency's mission.

(c) The Contractor shall provide, implement, and maintain a Continuation of Mission Critical Services Plan for continuing performance of services no matter the circumstances. The Plan shall describe the processes and procedures that will be followed to ensure continued availability of services under this contract. Any alternate site used as part of Disaster Recovery shall be fully operational within \_\_\_ TBD\_\_of a declared disaster.The Contractor shall identify in the Plan the provisions made for the acquisition of mission critical personnel and resources, if necessary, for continuity of operations for up to 30 days or until normal operations can be resumed.

(d) The offeror shall provide with its offer a written preliminary plan describing how it will continue to perform the contractor services listed in Attachment \_\_TBD \_\_\_, Mission Critical Contractor Services, dated \_\_TBD\_\_.

(e) Within \_\_ TBD\_\_ days after contract award, the Contractor shall submit its Plan for approval, which shall be consistent with and further detail the approach contained in the offeror's proposal. The Plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document. The Plan must, at a minimum, address:

1. Name of company’s officer overall responsible for the maintenance, management, exercising and execution of the Plan;
2. Plans and procedures;
3. Identification of mission critical functions;
4. The time lapse associated with the initiation of the acquisition of mission critical personnel and resources and their actual availability on site;
5. Delegations of authority, planned order of succession, and cross-training to ensure personnel are available to provide services and make key decisions;
6. Proposed alternate operating facilities, interoperable, connectivity and emergency communications approach;
7. Critical records or data storage procedures;
8. Protection of human capital;
9. Testing approach for \_\_TBD\_\_, annual tests a year;
10. Training plan;
11. Delegation of control and direction;
12. Reconstitution and resuming normal operations plans; and
13. Schedule for periodic review and revisions of Plan.

(f) The Contractor shall maintain and update its Plan as necessary and adhere to its requirements throughout the contract term. The Contractor shall not materially alter the Plan without the Contracting Officer's written consent.

(g) As directed by the Contracting Officer, the Contractor shall participate and collaborate with ED and its contractors in training events, exercises, and drills associated with Government efforts to test the effectiveness of continuity of operations procedures and practices with internal and external entities. Results of the exercises shall be delivered to the Contracting Officer or other designated representative within \_\_TBD\_\_ after the exercise.

(h) In the event the Contractor anticipates not being able to perform any of the mission critical contractor services identified in the paragraph above, the Contractor shall notify the Contracting Officer or other designated representative immediately and use its best efforts to cooperate with the Government in the Government's efforts to maintain the continuity of operations. In no way does (h) relieve the contractor of financial responsibility in meeting the contract terms and conditions.

(i) The Government reserves the right to use Federal employees of other agencies or support from other parties or to enter into new contracts for mission critical contractor services. Any new contracting efforts would be conducted in accordance with OFPP letter, “Emergency Acquisitions'' May 2011 and FAR Part 18, respectively, or any other subsequent emergency guidance issued.

(j) The Contractor shall include the substance of this clause, including this paragraph (j), in subcontracts for the mission critical services.

(End of clause)

**FSA 39-3 FSA Section 508 and Electronic and Information Technology Accessibility Standards Compliance (SEP 2016)**

(a) The performance of this contract is subject to the requirements of Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR Part 1194).

(b) Section 508 establishes requirements for electronic and information technology developed, maintained, procured, or used by the Federal government.  Section 508 requires Federal electronic and information technology, including that provided by a Government contractor, to be accessible to people with disabilities, including employees and members of the public.  All EIT services performed under this contract shall meet the standards identified at 36 CFR Part 1194 (<http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title36/36cfr1194_main_02.tpl>).

(c) Members of the public with disabilities that are seeking information or services from the contractor shall have access to and use of information and data maintained and provided to the public under this contract that is comparable to the access to and use of information and data by members of the public who are not individuals with disabilities.  The contractor’s Website, and any documents or other forms of communication that may be viewed by the public via the Website, shall remain current with manners of assistive technology utilized by the public for accessing such information.  In order to maintain an accessible Website and documents or other forms of communication, the contractor shall ensure that the public can access required information in a variety of ways, which do not have to rely on a single sense or ability of the user.

(End of Clause)

**FSA 39-4**  **Remedies for Contractor’s Violation of System Security Requirements (May 2017)**

1. General. The information systems accessed, supported, and maintained under this contract contains personally identifiable information (PII). In order to protect those systems and PII, the contractor is required by the terms of this contract to comply with the Department of Education security policy requirements and to implement privacy and security safeguards. A failure by the contractor to comply with those requirements that results in, or contributes to, a breach of an information system and to the improper disclosure of PII therein could negatively impact millions of student borrowers and their families, as well as many other individuals and entities. Such a breach could give rise to claims by third parties against the Department and the Department may incur significant additional costs and expenses. Depending on the number of systems and individuals affected and the sensitivity and amount of PII data involved in the breach, the Department’s liability, costs and expenses may include the following, among others: 1) costs of investigation of the system breach and its impact, 2) expenses related to notification of affected individuals, 3) costs of providing data breach protection services to affected individuals, 4) liability for financial and other losses suffered by third parties as a consequence of the fraudulent, negligent or other misuse of PII obtained as a result of the breach, and 5) expenses to restore Department systems to a state that ensures the present and future integrity, security and availability of PII.

(b) Definitions. All terms used in this provision such as breach, personally identifiable information (PII) have the same definition as used by the Department of Education’s Administrative Communications System Directive OM: 6-107 External Breach Notification Policy and Plan (3/25/2016).

(c) Breach Response. The contractor agrees that in the event of any actual or suspected breach of any system accessed, supported, and maintained under this contract and which contains or may contain PII, the contractor shall immediately, and in no event later than one hour of discovery, report the breach to the individuals identified in OCIO-14 Handbook for Information Security Incident Response and Reporting Procedures, contracting officer, the Contracting Officer’s Technical Representative (COTR), and the Department’s Privacy Advocate ([privacyadvocate@ed.gov](mailto:privacyadvocate@ed.gov)), and furnish a copy of the message to the contracting officer. The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. The contractor further agrees to provide the Department the resources necessary to support the Department in its implementation of appropriate information security incident response and reporting procedures and external breach notification policies and plans.

(d) Notice to Affected Individuals. If the contractor fails to comply with Department security policy requirements or fails to implement required privacy and security safeguards, in accordance with FSA’s instructions and only if and as approved in advance and in writing by the Department, the contractor agrees to prepare and send a notice to all individuals affected by a breach, at no additional cost to the Department. The method of such notification may include letters to affected individuals sent by first class mail, electronic means, or publication of a general notice, as approved by the Department. At minimum, that notification should include:

* 1. a brief description of how the breach occurred;
  2. a description of the types of personal information involved in the breach;
  3. a statement as to whether the information was encrypted or protected by other means;
  4. steps an individual may take to protect themselves;
  5. what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
  6. point of contact information identifying who affected individuals may contact for further information.

(e) Remedies for Violations. If the contractor fails to comply with Department security policy requirements or fails to implement required privacy and security safeguards, and if that failure results in, or contributes to, a breach of an information systems and the improper disclosure of PII, the contractor agrees to take all reasonable measures necessary to correct and mitigate the violation and to remedy any resulting harm suffered by the Department and any others. The contractor agrees to take such action promptly, as directed by the Contracting Officer, and at no additional cost to the Department. The contractor agrees that such measures shall include, at a minimum, the following:

* 1. the contractor shall provide data breach protection services, including identity theft and credit protection, to all affected individuals for a period of no less than 18 months from the date of discovery of the breach. Those services shall include at a minimum: a) one year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports; b) data breach analysis; c) fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; d) three years of identity theft insurance with up to $1,000,000.00 coverage at $0 deductible; and e) necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs;
  2. the contractor shall reimburse the Department for all its costs and expenses resulting from the breach, including but not limited to: a) costs of investigation of the system breach and its impact, b) expenses related to notification of affected individuals, c) costs of providing data breach protection services to affected individuals, d) expenses to restore Department systems to a state that ensures the present and future integrity, security and availability of PII;
  3. the contractor shall indemnify and hold harmless the Department for any and all third party claims, suits, demands, actions, causes of action, damages, set-offs, liens, attachments, debts, expenses, judgments, and any other liabilities of any kind or nature arising out of or related to the breach. This includes but is not limited to indemnification for any liability for financial and other losses suffered by third parties as a consequence of the fraudulent, negligent or other misuse of PII obtained as a result of the breach.

(f) Right to Withhold Contract Payments and Set-Off. If the contractor fails to notify the affected individuals or fails to provide the data breach protection services as provided in paragraphs (d) and (e)(1) of this clause, the contractor agrees to have the Department withhold the sum of $TBD per affected individual from any payment due the contractor under this contract, or to set-off that sum from any other Government contract. That withholding or set-off shall continue until the contractor has complied with the requirements in paragraphs (d) and (e)(1) of this clause. Should the Department elect to provide and/or procure notification or data breach protection services in response to a breach, the contractor will be responsible for reimbursing the Department for those expenses.

(g) Flow-Down to Subcontractors. The contractor agrees to incorporate into subcontracts at all tiers any term or condition necessary to ensure compliance with the requirements of this clause, including by contractor and subcontractor personnel. Further, the contractor acknowledges and agrees that a breach of an information system caused by subcontractor personnel will be attributed to the contractor for purposes of application of this clause.

*Reservation of Government Rights*. Nothing in this clause is intended or shall be interpreted to waive or to limit in any way the right of the Department to pursue claims and recover damages and other remedies for the contractor’s violation of the terms of this contract, including system security requirements.

(End of clause)

**FSA 39-5 Monthly Vendor Employee Report (AUG 2017)**

The Monthly Vendor Employee Report template (hereafter referred to as “report”) is included as an attachment to the contract. This report is a monthly deliverable under this contract. The contractor shall complete all fields of the report and provide timely delivery consistent with the instructions contained in the report.

(End of clause)

**FSA 39-6 Security Protocol for Reporting Contract Employee Departure from a Contract (SEP 2017)**

As part of Federal Student Aid’s security protocol, the contractor is required to provide timely notification of a contractor or subcontractor employee’s departure from the contract. All notifications of an employee’s departure are considered timely when the Contracting Officer, Contracting Officer’s Representative, and the Information System Security Officer are notified by the end of the business day of a contractor employee’s departure. All notifications shall be in the form of an encrypted email with a subject line of “Employee Departure.” The encrypted email shall include the following information:

* Employee Last Name, First Name, Middle Name
* eQIP number, if available
* Contract number
* List of systems to which the employee had access, and any associated user IDs, if available
* Termination date

The completion of this timely notification does not relieve the contractor of the inclusion of the same information in the monthly report in the format identified in FSA 39-5.

The content of this clause shall flow down to all subcontracts awarded under this contract.

(End of clause)

When responding to the Phase II solicitation(s), vendors will be required to register in the System for Award Management ([www.sam.gov](http://www.sam.gov)).

Attachments

|  |  |
| --- | --- |
| 01 | As-is |
| 02 | Vision |
| 03 | Technical Constraints Compendium |
| 04 | Attachments for Technical Constraints Compendium |
| 05 | Customer Journeys |
| 06 | Price Cost Template |
| 07 | Teaming Arrangement and Subcontracting Template |
| 08 | Question Template |

1. Links to existing servicer websites can be found at <https://studentaid.ed.gov/sa/repay-loans> [↑](#footnote-ref-2)