1. **How will the NCUA get this done?**
   - Buy vs. Build – An “off-the-shelf” technology will be selected where possible
   - Engage & Collaborate – Stakeholders will be given opportunities to provide input
   - Deploy Incrementally – Changes will be implemented in a disciplined and phased approach

2. **Why is the NCUA doing this?**
   - Support the NCUA’s mission of protecting consumers in an evolving financial services environment
   - Implement adaptable, flexible and secure technology that evolves with changes to regulations and the financial services industry
   - Streamline and align examination and data processes, technology, and infrastructure across the NCUA business functions
   - Improve process flexibility and adaptability to rapidly adjust to new regulatory processes, demands and priorities
   - Support the [Exam Flexibility Initiative](#)’s recommendations for a longer examination cycle, consistency between examiners, better communication, more efficient examination planning process, and better offsite monitoring tools.

3. **When will the solution(s) be implemented?**

   Deployment of the ESM solutions will occur in phases within a multi-year timeframe. We have a communications strategy and process to ensure all stakeholders are informed throughout the transition and will update this website and other communications as more information is available.

4. **How will the NCUA manage the complexity and impacts of this effort?**

   We have established the requisite programmatic policies, guidelines, and standard deployment process and organizational change management strategy, which includes:
   - Gathering and validating inputs from impacted employees and stakeholders;
   - Communicating status and impacts of the modernization throughout the transition; and
   - Offering comprehensive training to all users.
5. **Why is the NCUA considering purchasing Commercial Off-The-Shelf (COTS) solutions vs. building new tools?**

Although custom-built solutions offer unconstrained flexibility, the following summarizes the NCUA’s reasoning for considering the purchase of a solution vs. building a solution:

- **Cost** - Custom built solutions are the most expensive alternative. A COTS solution has an established framework and technical foundation that can be configured for the NCUA needs.
- **Expertise** – Custom built solutions require a high-level of in house support and expertise to build, deploy, and maintain. As a small agency, the NCUA can leverage the experts of a COTS solution for technical support.
- **Implementation Time** – Custom developed solutions are risky and typically take longer to implement due to the time required to design, build, document, and test. A more agile configuration approach of a COTS solution provides an opportunity to incrementally release functionality.
- **Technological Updates** – COTS solutions provide regular software and security updates that can be deployed with minimal user interruption.

Based on our market research, a COTS solution or set of solutions supports the strategic goals of achieving cost savings, reducing implementation time, and mitigating risk.

6. **What is the due diligence process for selecting a vendor(s)?**

The ESM Program Team’s approach includes the following actions before selecting the next generation examination tools and support services:

- Extended Market Research - To understand the full range of solutions available across the market place;
- Benchmarking - To provide insight and lessons learned from other organizations with similar business models; and
- Contract Competition - To assess a broad range of solutions (including in-depth evaluations of each product) and implementation strategies.

7. **What information security measures have been put in place?**

The NCUA exercises great care in protecting sensitive and personally identifiable information. As a federal agency, the NCUA must comply with mandatory security standards for federal information and information systems and must meet these minimum information security requirements by using security and privacy controls recommended by the National Institute of Standards and Technology.
(NIST). In addition to NIST standards and guidelines, the NCUA is subject to federal statutes such as the Federal Information Security Modernization Act (FISMA) of 2014, the E-Government Act of 2002, the Privacy Act of 1974 and various OMB policies and guidance concerning federal information management, FISMA reporting, and privacy.

The NCUA uses administrative, technical, and physical controls, including but not limited to: periodic review and authorization of information systems; proactive threat assessment and continuous monitoring; and annual general and role-based security training for employees and contractors. We also leverage independent tests and evaluations from other government agencies and third-party assessors.

The Office of the Inspector General (OIG) conducts independent audits, investigations and other activities to verify the NCUA’s compliance with applicable standards, laws and regulations related to privacy and information security and keeps the NCUA Board and U.S. Congress fully and currently informed of their work. The OIG conducts a FISMA and Federal Managers’ Financial Integrity Act (FMFIA) audit annually to ensure the NCUA has effectively implemented all appropriate security and privacy controls.