COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

OSCAR VALDEZ
AUDITOR-CONTROLLER

CONNIE YEE
CHIEF DEPUTY AUDITOR-CONTROLLER

NUMBER OF RECOMMENDATIONS	
PRIORITY 1	1
CORRECTIVE ACTION REQUIRED WITHIN 90 DAYS	
PRIORITY 2	4
CORRECTIVE ACTION REQUIRED WITHIN 120 DAYS	
PRIORITY 3	0
CORRECTIVE ACTION REQUIRED WITHIN 180 DAYS	

March 24, 2025

TO: Each Supervisor

FROM: Oscar Valdez
Auditor-Controller

Robert G. Campbell
Assistant Auditor-Controller / Chief Audit Executive

SUBJECT: **DEPARTMENT OF CHILDREN AND FAMILY SERVICES – SYSTEM DEVELOPMENT REVIEW**

With the support and active participation of the Department of Children and Family Services' (DCFS or Department) management, we evaluated the design of DCFS' system development processes and controls to determine whether they provide reasonable assurance to management that systems and applications are developed and implemented in accordance with County Fiscal Manual requirements and County Information Technology Standards.

We noted opportunities to improve DCFS' system development processes, controls, and control monitoring, which management has agreed to strengthen. For example:

- DCFS management will strengthen their system development processes by establishing documentation controls to provide evidence and assurance that staff identified and management approved and implemented all applicable system security requirements in new systems.

- DCFS management will enhance their end user training processes to ensure training is documented/logged to support all system users complete training prior to obtaining full system access.

These enhancements will strengthen system development operations and reduce the potential for exposure of sensitive County data, including protected health information.

For details of our review, see Attachment I. The Department's response, Attachment II, indicates general agreement with our findings and recommendations.

FAST FACTS

DCFS reported 23 systems in development (e.g., systems being developed in-house or acquired from third-party vendors), including the Incident Tracking System and Application.

DCFS also reported six critical systems that access, store, and/or transmit sensitive County or client data and are currently in operation.

We thank DCFS management and staff for their cooperation and assistance during our review. If you have any questions please call us, or your staff may contact Zoran Penich at zpenich@auditor.lacounty.gov.

OV:CY:RGC:ZP:mh

Attachments

c: Fesia A. Davenport, Chief Executive Officer
Edward Yen, Executive Officer, Board of Supervisors
Brandon T. Nichols, Director, Department of Children and Family Services

LOS ANGELES COUNTY
AUDITOR-CONTROLLER

Robert G. Campbell ASSISTANT AUDITOR-CONTROLLER	**Zoran Penich** CHIEF ACCOUNTANT-AUDITOR

AUDIT DIVISION

Report #K23FC

DEPARTMENT OF CHILDREN AND FAMILY SERVICES
SYSTEM DEVELOPMENT REVIEW

BACKGROUND

The Department of Children and Family Services (DCFS or Department) is responsible for ensuring the safety and well-being of more than two million children across Los Angeles County. DCFS staff rely on their systems to provide children and family support services and specialized programs, including six critical systems that maintain sensitive information, such as protected health information (PHI) and personally identifiable information (PII). At the time of our review, DCFS reported 23 systems in development to enhance and support critical departmental operations. This includes customized systems being developed internally, such as DCFS' Education Specialist Referral System (ESRS) and Incident Tracking System and Application (iTrack), and systems acquired from third-party vendors.

We evaluated the design of DCFS' system development processes and controls to determine if they provide reasonable assurance to management that systems are developed and implemented in accordance with County Fiscal Manual (CFM) requirements and County Information Technology (IT) Standards and Directives. We reviewed processes and controls, including management monitoring, for defining system requirements, including County IT and security requirements; designing systems, including developing, testing, and approving systems for implementation; and implementing systems, including providing end-user training and employing appropriate deployment strategies. Our review was not intended or designed to ensure the 23 new systems were being properly developed, but only to assess whether DCFS' processes and controls for developing systems provide reasonable assurance in that regard.

Based on our interviews, walkthroughs, and review of documentation, we noted DCFS established processes and controls to reasonably ensure systems are appropriately tested and approved prior to deployment. However, we also identified opportunities for improvement as noted in the table below.

TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION

	ISSUE	RECOMMENDATION
1	**System Security Requirements** - Departments need processes to identify and document system security requirements for new systems to ensure systems and their data are properly protected. These processes are required by County Fiscal Manual (CFM) Section 8.5.0 and the Chief Information Security Office's (CISO) Application and Database Security Standard. We noted DCFS has various processes to help ensure systems in development meet County security requirements. However, the Department needs to improve their processes to ensure that all security requirements are properly identified and addressed. Specifically:	**Priority 1 - DCFS management strengthen their processes to ensure systems in development meet County security requirements by establishing documentation controls, such as requirements to maintain annotated checklists, to provide evidence and assurance that staff identified and management approved and implemented all applicable security requirements in the new system.** **Department Response: Agree** Implementation Date: March 31, 2025

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION	
	ISSUE	**RECOMMENDATION**
	• DCFS requires staff to review departmental security policies in the planning phase to identify security requirements applicable to the new system, and for management to ensure the new system includes these requirements before approving the next phase of system development. Examples of system security requirements could include user access controls and end-to-end encryption. However, DCFS does not have documentation controls, such as a security requirements checklist, e-mails, and/or memos, to provide evidence and assurance that staff identified and management approved all security requirements. • DCFS requires staff to work with the Internal Services Department to perform vulnerability scans that ensure the newly developed systems include the security requirements identified in the planning phase. While DCFS management maintains documented vulnerability scan results, they do not have documentation controls, such as requirements to compare and annotate security requirements checklists with scan results, to provide evidence and assurance that they implemented all security requirements identified during the planning phase. **Impact:** While vulnerability scans typically address standard County security requirements, these weaknesses increase the risk that not all applicable County and/or departmental security standards are implemented in new systems, including the 23 systems DCFS currently has in development. This may lead to system vulnerabilities and the potential exposure of sensitive DCFS data the systems may use.	
2	**End-User Training** - Departments need processes to ensure system users are adequately trained on their assigned functions before being granted system access. Training should be formalized and documented to support training completion. These controls are required by CFM Sections 8.3.1, 8.5.0, and 8.5.2.4. We noted DCFS has a process to develop training programs and materials, and conduct end-user	**Priority 2 - DCFS management enhance their training processes by establishing controls, such as a mechanism to track training assignments and participation, to ensure all system users complete training before being granted system access.** **Department Response: Agree** Implementation Date: July 31, 2025

	TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION	
	ISSUE	**RECOMMENDATION**
	training for new systems. Specifically, DCFS requires system development staff to develop formal system training upon completion of the system and provide the training materials and any technical assistance to the Training Division. DCFS also requires the Training Division to train users on their assigned functions/capabilities before being granted system access. However, the Department does not have controls to ensure users complete training. Controls could include a mechanism to track training assignments and participation, such as a sign-in log of all required users. **Impact:** This weakness increases the risk that users will not be adequately trained to perform system tasks/functions, potentially resulting in erroneous actions, loss of information, and/or delay of services to DCFS' clients and related agencies.	
3	**System Deployment Strategy** - Departments need processes to evaluate and select system deployment strategies that minimize risk and ensure a successful transition, as required by CFM Section 8.5.0. These processes help ensure departments compare the benefits and costs of each system deployment approach (e.g., immediately replacing the old system with the new, or gradually implementing the new system in stages) with the risks and costs of potential deployment issues. They also help document a clear roadmap for transitioning a new system into operation. DCFS requires management to evaluate and approve deployment strategies for new systems during system development. Department management indicated that they work with stakeholders to determine the most appropriate deployment method and timeline, but typically employ a direct deployment strategy (i.e., immediate full implementation of new system and processes) and perform system rollbacks if they encounter issues (i.e., restore previous systems and files). Management also verbally approves the deployment strategy during project meetings. However, there is no documented evidence or assurance to support the evaluation, selection, and approval.	**Priority 2 - DCFS management strengthen their system deployment process by establishing documentation controls, such as meeting minutes and/or e-mails, to support:** **a) Their deployment strategy evaluation and selection, including factors considered, such as deployment risk/cost, stakeholder input, and rollback plans.** **b) Management's review and approval of the system deployment strategy.** **Department Response: Agree** Implementation Date: April 1, 2025 The Department's response does not directly address the portion of our recommendation related to documenting consideration of factors such as deployment risk/cost and stakeholder input, in their deployment strategies. However, we confirmed with DCFS management that their corrective action will incorporate these factors. We will assess and report on the details of the Department's implementation during our six-month follow-up review.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION	
	ISSUE	**RECOMMENDATION**
	DCFS should establish documentation controls to provide evidence and assurance of this activity. Controls could include requirements to document in meeting minutes, e-mail, and/or project documents: • Their deployment strategy evaluation and selection, including factors considered, such as deployment risk/cost, stakeholder/end-user input, and plans to perform rollbacks in the event of any issues during deployment. • Management's review and approval of the deployment strategy. **Impact:** These weaknesses increase the risk of ineffective and/or inefficient system deployment, which may result in system malfunction and downtime, and delays or interruptions in services.	
4	**Management Monitoring of Controls** - DCFS needs to develop ongoing self-monitoring processes to regularly evaluate and document that the following processes and controls are working as intended, as required by Board of Supervisors Policy 6.100 and CFM 1.0.2: • Documenting system security requirements, as noted in Issue No. 1. • End-user training, as noted in Issue No. 2, and that training programs are established for all systems developed. • System deployment strategies, as noted in Issue No. 3. Effective self-monitoring processes could include tests or observations examining an adequate number of transactions on a regular basis (e.g., 5 -10 weekly, quarterly, semi-annually) to ensure adherence to County policy, rules, and/or generally accepted control principles, and documenting and retaining evidence of this review in a manner that a third-party can subsequently validate. The monitoring process should also ensure material exceptions are elevated timely so management is informed of control risks and can take appropriate actions.	**Priority 2 - DCFS management develop ongoing self-monitoring processes that include:** **a) Examining process and control activities, such as reviewing an adequate number of transactions on a regular basis to ensure adherence to County information technology rules.** **b) Documenting the monitoring activity and retaining evidence so it can be validated.** **c) Elevating material exceptions timely so management is aware of control risks and can take appropriate corrective actions.** **Department Response: Agree** Implementation Date: July 31, 2025

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

	TABLE OF FINDINGS AND RECOMMENDATIONS FOR CORRECTIVE ACTION	
	ISSUE	**RECOMMENDATION**
	Impact: Weaknesses in management self-monitoring processes prevent management from having reasonable assurance that important departmental and County system development objectives are being achieved. This also increases the risk for not promptly identifying and correcting process/control weaknesses or instances of non-compliance with County rules.	
5	**Standards and Procedures** - DCFS needs to develop written standards and procedures to adequately guide supervisors and staff in the performance of their duties for the following processes, as required by CFM Section 8.3.0: • Defining system security requirements, as noted in Issue No. 1. • End-user training, as noted in Issue No. 2. • System deployment strategies, as noted in Issue No. 3. • Self-monitoring processes, as noted in Issue No. 4. Standards and Procedures should provide detailed guidance to staff and supervisors in the performance of their day-to-day duties and describe how processes are performed. **Impact:** The lack of written standards and procedures increases the risk that staff will perform tasks incorrectly or inconsistently and prevent management from effectively evaluating processes and controls.	**Priority 2 - DCFS management develop written standards and procedures to guide supervisors and staff in performing system development duties.** **Department Response: Agree** Implementation Date: July 31, 2025

We conducted our review in conformance with the International Standards for the Professional Practice of Internal Auditing. For more information on our auditing process, including recommendation priority rankings, the follow-up process, and management's responsibility for internal controls, visit auditor.lacounty.gov/audit-process-information.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

County of Los Angeles
DEPARTMENT OF CHILDREN AND FAMILY SERVICES
510 S. Vermont Avenue, Los Angeles, California 90020
(213) 351-5602

BRANDON T. NICHOLS
Director

JENNIE FERIA
Chief Deputy Director

March 13, 2025

To: Oscar Valdez
Auditor-Controller

From: Brandon T. Nichols
Director

RESPONSE TO THE AUDITOR-CONTROLLER'S DEPARTMENT OF CHILDREN AND FAMILY SERVICES – SYSTEM DEVELOPMENT REVIEW

Attached is the Department of Children and Family Services' (DCFS) response to the findings and recommendations contained in the Auditor-Controller's (A-C) System Development Review. DCFS is in agreement with and has initiated appropriate corrective actions to address the recommendations contained in your report. We appreciate the opportunity to include our response in your report and thank your A-C staff for their professionalism and objectivity during this review.

If you have any questions or require additional information, please have your staff contact Nancy Neville, Head Compliance Officer, at (323) 881-1509.

BTN:JF:CMM:RH

Attachment

c: Cynthia McCoy-Miller, Senior Deputy Director
Rae Hahn, Departmental Chief Information Officer
Allen Ohanian, Departmental Information Security Officer

DEPARTMENT OF CHILDREN AND FAMILY SERVICES – SYSTEM DEVELOPMENT REVIEW
DEPARTMENT ACTION PLAN/RESPONSE

ISSUE 1: SYSTEM SECURITY REQUIREMENTS	
A/C Recommendation	DCFS management strengthen their processes to ensure systems in development meet County security requirements by establishing documentation controls, such as requirements to maintain annotated checklists, to provide evidence and assurance that staff identified and management approved and implemented all applicable security requirements in the new system.
Priority	**PRIORITY 1**
Agree/Disagree	**Agree**
Department Action Plan[1]	The Department agrees and acknowledges that there is an opportunity to further enhance our documentation controls as it relates to system security requirements that align with this recommendation. It is important to note that DCFS enforces a zero-tolerance policy for security vulnerabilities, ensuring that every system meets the highest standards of cybersecurity before deployment. Security is integrated into every stage of the system development lifecycle, and while compliance with documentation is an important aspect of the overall strategy, real security is achieved through continuous testing, validation and proactive risk mitigation. This layered approach ensures that risk is reduced to near zero. Every application undergoes a multi-tiered security assessment process that combines automated vulnerability scans with rigorous manual reviews. A leading industry vendor performs these automated scans in full alignment with the OWASP Top 20, NIST guidelines and other industry best practices, while expert-led manual assessments including penetration testing and code reviews address any issues that automated tools might miss. This dual methodology guarantees that no vulnerabilities remain unaddressed before an application is cleared for deployment. DCFS maintains dynamic security measures that are continuously updated. Applications are not only thoroughly tested prior to deployment but are also subject to frequent patching and re-assessments to address emerging threats. Strict patch management protocols, as detailed in the DCFS PATCH MANAGEMENT PROCEDURE, ensure that any identified vulnerabilities are mitigated in a timely manner, reinforcing the commitment to continuous improvement. Once an application is approved for production, it is immediately placed behind the County's Web Application Firewall (WAF), which offers real-time monitoring, traffic filtering, and automated threat detection. This additional layer of defense protects against common web-based attacks such as SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks. Post-deployment security is further enhanced through ongoing monitoring, incident response capabilities, and forensic analysis to swiftly address any new threats. DCFS' security framework is supported by a comprehensive suite of documented standards and procedures: • The DCFS App Security Standard Integrated delineates the secure coding practices, threat modeling, and design requirements that the development team must incorporate from the outset.

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

ISSUE 1: SYSTEM SECURITY REQUIREMENTS	
	• The County Network Vulnerability Scanning Standards specifies the technical parameters and frequency for automated scans, ensuring consistency and thoroughness in security assessments. • The DCFS Vulnerability Management Program, along with the accompanying Vulnerability Management Directive, establishes a clear process for identifying, logging and remediating security issues. • The WH Sectional Policy and Monitoring Protocol for WhiteHat eLearning Training further ensures that development personnel remain current with evolving cybersecurity best practices through mandatory, ongoing training. In practical terms, the development team is required to integrate secure coding practices and threat modeling into every phase of the development process as specified in the DCFS App Security Standard Integrated. Developers must conduct automated vulnerability scans using approved tools that comply with the County Network Vulnerability Scanning Standards and follow these scans with comprehensive manual security reviews and penetration testing to identify any issues not captured by automation. All applications must be completely free of vulnerabilities before deployment, with strict adherence to the patch management process outlined in the DCFS PATCH MANAGEMENT PROCEDURE, ensuring that any identified issues are tracked, prioritized, and remediated promptly. Furthermore, all security controls, testing outcomes, and remediation efforts must be thoroughly documented in accordance with the guidelines outlined in the DCFS Vulnerability Management Program and Directive, thereby supporting auditability and continuous improvement. The development team is also required to complete regular cybersecurity training through the WhiteHat eLearning platform to remain informed about emerging threats and mitigation strategies. Coordination with the Internal Services Department (ISD) is essential to ensure that all security testing and monitoring processes are continuously evaluated and updated in response to evolving cybersecurity challenges. By mandating zero vulnerabilities, enforcing multiple layers of security testing, and deploying applications behind state-of-the-art security infrastructure, DCFS ensures that its systems are resilient, secure, and among the most robust in county operations. This comprehensive and continuously evolving approach dramatically reduces risk and provides a high level of assurance against potential vulnerabilities. Nevertheless, the Department used this review as an opportunity to further enhance the security of DCFS systems and applications by instituting a security checklist. Before deployment and upon completion of the programming code, development teams are required to complete an annotated security checklist. This checklist ensures that all security requirements have been addressed and provides verification of compliance with DCFS's policies. It is reviewed and approved by the Information Security Officer or designee to independently confirm adherence to security standards.
Planned Implementation Date	3/31/2025
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

ISSUE 2: END USER TRAINING	
A/C Recommendation	DCFS management enhance their training processes by establishing controls, such as a mechanism to track training assignments and participation, to ensure all system users complete training before being granted system access.
Priority	**PRIORITY 2**
Agree/Disagree	Agree
Department Action Plan[1]	The Department agrees and is currently adhering to the processes for tracking training assignments that align with this recommendation. Nevertheless, the Department acknowledges there is always an opportunity to enhance our mechanisms for tracking system trainings. BIS has implemented processes to improve program staff readiness by ensuring program staff are adequately trained to perform system tasks/functions prior to being granted system access. These methods include, but are not limited to: • Identifying Executive Sponsors/Program Leads; • Establishing clear BIS and Program responsibilities; • Utilizing a train-the-trainer model and knowledge transfer sessions; and • Developing user guides, training videos, etc. as appropriate. To further enhance our processes and comply with the audit findings, BIS will collaborate with the Policy Section to develop a management directive whereby these controls, policies and procedures will be documented for implementation.
Planned Implementation Date	7/31/2025
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

ISSUE 3: SYSTEM DEPLOYMENT STRATEGY	
A/C Recommendation	DCFS management strengthen their system deployment process by establishing documentation controls, such as meeting minutes and/or e-mails, to support: a) Their deployment strategy evaluation and selection, including factors considered, such as deployment risk/cost, stakeholder input, and rollback plans. b) Management's review and approval of the system deployment strategy.
Priority	**PRIORITY 2**
Agree/Disagree	Agree

Department Action Plan[1]	The Department agrees and is currently adhering to the process for deploying systems that align with this recommendation. Nevertheless, the Department acknowledges there is always an opportunity to enhance our document controls as it relates to system deployment. BIS currently ensures that DCFS management evaluates and approves deployment strategies for new systems. To further comply with the audit findings, BIS will be implementing a System Deployment Strategy, which will establish documentation controls to provide evidence and assurance of this activity. Specifically, the documentation controls will be comprised of a Deployment Plan Checklist and Development Rollback Checklist that will at a minimum capture the following activities and data components:
	
	• Deployment Plan Checklist
	  ○ Create deployment schedule;
	  ○ Create and prepare database implementation scripts and rollback scripts;
	  ○ Prepare all .NET code and dependencies;
	  ○ Complete deployment run through on production database;
	  ○ Create new code branch;
	  ○ Establish communication channels with the Help Desk;
	  ○ Application name, version number and server name;
	  ○ DevOps Project Manager Lead and Application Developer Lead; and
	  ○ Date.
	• Development Rollback Checklist
	  ○ The directive to the development staff to create a backup;
	  ○ The directive to the development staff to do a rollback if an issue identified;
	  ○ Application name, version number and server name;
	  ○ DevOps Project Manager Lead and Application Developer Lead; and
	  ○ Date.
	
	Upon completion of the System Deployment Strategy, the documents will be made available for DCFS Management review and retained in a centralized repository, similar to what BIS utilizes for the logging and storing of its codes/test scripts, for historical record keeping purposes.

Planned Implementation Date	4/1/2025
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

ISSUE 4: MANAGEMENT MONITORING OF CONTROLS	
A/C Recommendation	DCFS management develop ongoing self-monitoring processes that include: a) Examining process and control activities, such as reviewing an adequate number of transactions on a regular basis to ensure adherence to County information technology rules. b) Documenting the monitoring activity and retaining evidence so it can be validated. c) Elevating material exceptions timely so management is aware of control risks and can take appropriate corrective actions.
Priority	**PRIORITY 2**
Agree/Disagree	**Agree**
Department Action Plan[1]	The Department agrees and will be implementing self-monitoring processes that align with this recommendation. The Department further acknowledges the opportunity to enhance our Management Monitoring of Controls as it relates to the following findings identified in this report: • System Security Requirements; • Train-the-trainer Training; and • System Deployment Strategies. As such and on an annual basis, BIS Management will identify a manager external to each of the aforementioned processes who will ensure the effective examining, documenting and monitoring of process and control activities.
Planned Implementation Date	**7/31/2025**
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.

ISSUE 5: STANDARDS AND PROCEDURES	
A/C Recommendation	DCFS management develop written standards and procedures to guide supervisors and staff in performing system development duties.
Priority	PRIORITY 2
Agree/Disagree	Agree
Department Action Plan[1]	The Department agrees and will be implementing a process that aligns with this recommendation. The Department further acknowledges the opportunity to enhance our Standards and Procedures as it relates to the following findings identified in this report: • System Security Requirements; • Train-the-trainer Training; and • System Deployment Strategies. As such, BIS Management will develop and update existing documentation providing written standards and procedures to help and guide managers, supervisors and staff in the performance of their duties pertaining to the aforementioned processes. To further comply with this finding, BIS Management will establish a centralized repository to house material evidence (e.g., documents, checklists, etc.) for DCFS Management review and retain, as appropriate, for historical record keeping and validation purposes.
Planned Implementation Date	7/31/2025
Additional Information (optional)[2]	

[1] In this section the Department should only describe the efforts they plan to take to implement the recommendation. Any other information should be included in the Additional Information section below.
[2] In this section the Department can provide any background or clarifying information they believe is necessary.

Priority Ranking: Recommendations are ranked from Priority 1 to 3 based on the potential seriousness and likelihood of negative impact on the Agency's operations if corrective action is not taken.