May 1, 2024

Re: NIST 800-53 Attestation Letter

To Whom It May Concern:

Softdocs SC, LLC (Softdocs) engaged KirkpatrickPrice to perform an audit of their services based on NIST (National Institute of Standards and Technology) Special Publication 800-53. Our overall internal audit revealed that Softdocs has adequately addressed the significant security requirements deemed necessary for a "moderate-impact" system.

Based on our objective analysis, we determined that Softdocs has implemented safeguards that meet the protections required by NIST 800-53, and the information security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected as of February 16, 2024.

The following security controls were in scope for this engagement:

1. AC - Access Control (Technical)
2. AT - Awareness and Training (Operational)
3. AU - Audit and Accountability (Technical)
4. CA - Security Assessment and Authorization (Management)
5. CM - Configuration Management (Operational)
6. CP - Contingency Planning (Operational)
7. IA - Identification and Authentication (Technical)
8. IR - Incident Response (Operational)
9. MA - Maintenance (Operational)
10. MP - Media Protection (Operational)
11. PE - Physical and Environmental Protection (Operational)
12. PL - Planning (Management)
13. PS - Personnel Security (Operational)
14. RA - Risk Assessment (Management)
15. SA - System and Services Acquisition (Management)
16. SC - System and Communication Protection (Technical)
17. SI - System and Information Integrity (Operational)

About Softdocs

Softdocs provides process automation and document management solutions to schools, states, counties, and cities. Softdocs' secure SOC 2 Type II compliant SaaS offerings enable colleges, universities, K-12 school districts, and state and municipal governments to improve how they serve people, create new efficiencies, and enable the future of work. Softdocs solutions are used by nearly one thousand organizations.

About NIST 800-53

Organizations are required to adequately mitigate the risk arising from the use of information and information systems in the execution of business functions. A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost effectively mitigate risk while complying with the security requirements defined by applicable federal laws, executive orders, directives, policies, standards, or regulations.

Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53, Rev. 4. This allows organizations to tailor the relevant security control baselines to align with their mission and business requirements and their environments of operation more closely. Security controls as defined in the NIST security control baselines represent an information system-wide set of controls that may not be necessary or applicable to every component in the system.

Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of the potential risk being mitigated by the control. For example, auditing controls are typically allocated to components of an information system that provide auditing capability (e.g., servers) and are not necessarily applied to every user-level workstation within the organization. Organizations must assess the inventory of information system components to determine which security controls are applicable to the various components and subsequently make explicit decisions regarding where to allocate the controls to satisfy the organizational security requirements.

KirkpatrickPrice performed its internal audit based on an approach in which all systems and related processes were categorized as "moderate-impact." Through collaborative evaluation with Softdocs' executive management, we classified the Softdocs information system as a moderate-impact system and evaluated controls against the corresponding moderate-impact security control baselines defined in NIST SP 800-53, Rev. 4.

Deliverable Summary

KirkpatrickPrice is engaged to issue the following deliverables to Softdocs as part of the assessment:

- Phase 1
    - o Asset Characterization
    - o Risk Assessment
- Phase 2
    - o System Security Plan
- Phase 3
    - o Remediation Plan
    - o NIST 800-53 Report

If you have any questions, please don't hesitate to reach out to us.

Sincerely,

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA