IF-352
(Rev. 11/23)

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

WASHINGTON, D.C. 20544

Date: 07/19/2024

GUIDE TO JUDICIARY POLICY

TRANSMITTAL	14-023	**VOLUME/PART**	14	**CHAPTER(S)**	1, 2

TO: Circuit Executives
Federal Public/Community Defenders
District Court Executives
Clerks, United States Courts
Chief Probation Officers
Chief Pretrial Services Officers
Circuit Librarians
Bankruptcy Administrators
Certified Contracting Officers

FROM: Judge Robert J. Conrad, Jr. Robert J Conrad Jr
Director

RE: **PROCUREMENT**

This transmittal provides notice of changes to *Guide to Judiciary Policy*, Volume 14 (Procurement):

Appendix 1B – Solicitation Provisions and Contract Clauses
Appendix 1C – Matrix of Solicitation Provisions and Clauses (Including Key)
Chapter 2 – Procurement Planning and Preparations

This update adds an IT-related clause addressing potential cyber incidents in which personally identifiable information (PII) and sensitive personally identifiable information (SPII) is breached, exposed, exfiltrated, or stolen, by providing contractors and their subcontractors with: guidance and requirements on the handling and protection of sensitive information, guidance on reporting and responding to incidents, and requiring notification and credit monitoring services when directed by the contracting officer. The significant changes are detailed in the Redline Comparison below.

Questions regarding this transmittal may be directed to the Procurement Management Division of the AO's Department of Administrative Services, at 202-502-1330.

REDLINE COMPARISON REFLECTING CHANGES

[Significant changes in Appendix 1B (Solicitation Provisions and Contract Clauses) follow:]

Clause 2-57, Protecting, Reporting, and Responding to Incidents Involving Sensitive Information

~~Clause 2-60, Stop-Work Order~~

Include the following clause as prescribed in § 220.25.80(c) (Service-Related Provisions and Clauses).

Protecting, Reporting, and Responding to Incidents Involving Sensitive Information (JUN 2024)

(a) Definitions. As used in this clause—

“Breach” means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where an unauthorized person accesses or potentially accesses Sensitive Information, or an authorized user accesses Sensitive Information for an unauthorized purpose.

“Incident” means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation, or imminent threat of violation, of law, security policies, security procedures, or acceptable use policies.

“Information System” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Personally Identifiable Information (PII)” means information that can identify an individual, when used alone or with other relevant data. PII may contain direct identifiers (e.g., Social Security numbers) that can identify a person uniquely or quasi-identifiers (e.g., date of birth) that can be combined with other quasi-identifiers to successfully recognize an individual. The definition of PII is not anchored to any single category of information or technology. Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

“Privacy Information” means both PII and Sensitive Personally Identifiable Information (SPII).

“Sensitive Information” means any data or other information for which public disclosure, or disclosure to users without a need to know to perform their jobs, can harm individuals, the U.S. government, or private organizations. Sensitive Information includes Privacy Information and the following types of information:

(1) Agreement Information. Information received by judiciary organizations, according to agreements with other federal, state, local, tribal, territorial, or private sector partners, that is required to be protected under the agreement with that partner or other applicable laws.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(2) Procurement Information. Information related to procurements that is considered sensitive and is not normally shared with the public outside official processes. This includes internal information and documents related to procurements, source selection information, vendor proposals, and submitted information marked as proprietary or sensitive. This does not include the contractor's own proposal(s) or contract(s) with the judiciary.

(3) Information Systems Vulnerability Information (ISVI).

(A) Information technology (IT) systems data (e.g., systems inventories, enterprise architecture models) that reveal infrastructure used for servers, desktops, and networks; application name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use or need.

(B) Information about developing or current technology, the release of which could hinder judiciary objectives, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

(C) System vulnerability or weakness information that could be used to compromise the confidentiality, integrity, or availability of an information system.

(4) Personnel Security Information. Information that could result in physical risk to judiciary personnel.

(5) Physical Security Information. Information related to the protection of judiciary buildings, grounds, or property, including reviews or reports that illustrate or disclose facility infrastructure or security vulnerabilities. Examples include threat assessments, system security plans, security diagrams for judiciary buildings, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation.

(6) Court Related Information. Sealed cases, sealed documents or other information marked as sensitive by a court. This includes Highly Sensitive Documents (HSD), which are documents or other materials that contain sensitive, but unclassified, information that warrants exceptional handling and storage procedures to prevent significant consequences from unauthorized access or disclosure.

(7) Privileged/confidential Information. Information protected through recognized confidential relationships.

(8) Official Business Information. Proposed budgets, draft plans or policies, other information intended only for consideration by internal decision makers or other confidential audiences.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(1) Multiple pieces of information, when combined, may pose an increased risk of harm to the individual. SPII may consist of any grouping of information that contains an individual's name or other unique identifier, plus one or more of the following elements:

(A) Truncated SSN (e.g., last four digits);

(B) Birthdate (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information (e.g., mother's birth name, account passwords, personal identification numbers (PINs)).

(2) Other PII (e.g., list of employees and their performance ratings, unlisted home address, unlisted phone number) that may present an increased risk of harm to the individual depending on its context. The context includes the purpose for which the PII was collected, maintained, and used. The same information in different contexts can reveal additional information about the impacted individual.

(b) Accessing and Protecting Sensitive Information

(1) Contractor roles and responsibilities regarding Sensitive Information. Before the contractor shall have access to Sensitive Information, the contractor shall coordinate with the contracting officer's representative (COR) about the contractor's roles and responsibilities regarding the Sensitive Information, and how an incident or suspected incident will be handled consistent with this clause and judiciary policies and procedures. Before they may access the Sensitive Information, the contractor, their staff, and subcontractors shall complete all forms, trainings, and briefings as may be necessary for security or other reasons.

(2) Training. Contractors that have access to Sensitive Information as part of this contract shall provide their staff with training before they access Sensitive Information, and then at least annually thereafter. The training shall comply with this clause and the training shall cover how to properly handle and safeguard judiciary Sensitive Information and how to identify and report incidents or suspected incidents regarding judiciary Sensitive Information consistent with this clause. The contractor shall provide an initial report, and then an annual report each year after that, to the COR that shows that contractor staff and any subcontractor staff working on the contract have all successfully completed such training. The Contractor shall also provide the COR confirmation that any new staff or subcontractor staff that join the contract after the contract has begun have also successfully completed such training.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(3) Access. Contractor shall have access only to those areas of judiciary Sensitive Information resources explicitly stated in this contract or approved by the contracting officer or COR in writing, as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the contracting officer or COR, are strictly prohibited. If this clause is violated, the judiciary will take appropriate actions regarding the contract and the individual(s) involved.

(4) Protection Requirements

(A) Contractor shall safeguard all Sensitive Information and shall take reasonable measures to prevent the unauthorized use, disclosure, or loss of Sensitive Information. This includes Sensitive Information in any medium or form, including electronic, oral, or paper.

(B) Contractor and their subcontractors shall safeguard Sensitive Information whether it resides on judiciary owned and operated information systems, judiciary owned and contractor-operated information systems, contractor-owned and/or operated information systems operating on behalf of the judiciary, and any situation where contractor and/or subcontractor employees may have access to Sensitive Information because of their relationship with the judiciary.

(C) Sensitive Information shall not be stored on a mobile device or portable electronic media and shall be handled with awareness of the surroundings, so that the Sensitive Information is not disclosed to unauthorized individuals. Sensitive Information shall be secured when unattended or not in use. If performance of the contract requires the contractor to access Sensitive Information on a mobile device or portable electronic media, they shall notify the contracting officer and COR and provide details on the use case required and how such use will comply with this clause and all other applicable policies and guidelines. The COR will work with the contractor and determine if such a use case is acceptable. The contractor shall not use or store Sensitive Information on a mobile device or portable electronic media until the contracting officer provides acceptance of the use case.

(D) Contractor shall encrypt Sensitive Information if the Sensitive Information is in transit or is stored outside of judiciary networks. This includes any Sensitive Information that may reside on, or transit contractor-owned or operated information systems.

(E) All Sensitive Information must be appropriately labeled, secured, and be properly returned, disposed of, or sanitized when no longer needed or at the end of the contract. See section (e) of this clause for more guidance on returning, sanitizing, and disposing of judiciary Sensitive Information.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(F) Removal. The contracting officer may require the contractor to prohibit individuals from working on the contract if the judiciary deems their initial or continued employment on the contract contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(c) Incident Reporting Requirements

(1) Contractors and subcontractors shall report all known or suspected incidents to the Security Operations Center (SOC), which is staffed 24 hours per day, seven days per week.

(A) When reporting incidents to the SOC, contractors and subcontractors shall submit the report by:

(i) email to soc@ao.uscourts.gov with courtesy copy to the contracting officer and COR using the contact information identified in the contract, or

(ii) phone call to **202-502-4370**, in which case the contractor must notify the contracting officer and COR immediately after reporting to the SOC.

(B) Contractors and subcontractors shall report all known or suspected incidents involving PII or SPII within one hour of discovery. All other incidents shall be reported within eight hours of discovery.

(C) Subcontractors shall notify the prime contractor if they have reported a known or suspected incident to the SOC. Lower tier subcontractors shall also notify their higher tier subcontractor, until the prime contractor is reached.

(2) The judiciary will determine whether information exposed in an unauthorized disclosure or security breach of information under the contractor's control or in an information system under the contractor's control at the time of the incident is Sensitive Information, PII, or SPII by performing an assessment of the specific risk that an individual could be identified using the exposed information with other information that is linked or linkable to the individual. Information that is not PII when considered alone can become PII or SPII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to an individual. Final determination of the categorization of exposed information as Sensitive Information, PII, or SPII will be made in writing by the contracting officer.

(3) Sensitive Information transmitted via email shall be protected by encryption. When using regular email channels, contractors and subcontractors shall not include any Sensitive Information in the subject or body of any email. The Sensitive Information shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of Sensitive Information shall comply with any email restrictions imposed by the originator.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(4) No incident may, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate information security safeguards for Sensitive Information or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, contractors and subcontractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(A) Unique Entity Identifier (UEI);

(B) Contract numbers affected, unless all contracts by the company are affected;

(C) Facility CAGE code, if the location of the event is different than the prime contractor location;

(D) Point of contact (POC), if different than the POC recorded in the System for Award Management (address, position, telephone, and email);

(E) Contracting officer POC (address, telephone, and email);

(F) Contract clearance level;

(G) Name of subcontractor and CAGE code, if this was an incident on a subcontractor network;

(H) Government programs, platforms, or systems involved;

(I) Location(s) of incident;

(J) Date and time the incident was discovered;

(K) Server names where Privacy Information resided at the time of the incident, both at the contractor and subcontractor level;

(L) Description of the government PII or SPII contained within the system; and

(M) Any additional information relevant to the incident.

(d) Incident Response Requirements

(1) All determinations by the judiciary related to incidents, including response activities, will be made in writing by the contracting officer.

(2) The contractor shall provide full access and cooperation for all activities determined by the government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(3) Incident response activities determined to be required by the government may include, but are not limited to, the following:

(A) Inspections;

(B) Investigations;

(C) Forensic reviews;

(D) Data analyses and processing; and

(E) Revocation of the Authority to Operate (ATO), if applicable.

(4) The contractor shall immediately preserve and protect images of known affected information systems and all available monitoring or packet capture data. The monitoring or packet capture data shall be retained for at least 180 days from submission of the incident report to allow the judiciary to request the media or decline interest.

(5) The judiciary, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information

Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the contractor shall return all Sensitive Information to the judiciary and/or destroy it physically and/or logically as identified in the contract, unless the contract states that return and/or destruction of Sensitive Information is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The contractor shall submit the certification to the COR and contracting officer following the template provided in NIST SP 800–88, Guidelines for Media Sanitization, Appendix G.

(f) Other Reporting Requirements

Incident reporting required by this clause does not rescind the contractor's responsibility for other incident reporting pertaining to its information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other government requirements.

(g) PII and SPII Incident Notification Requirements

(1) All determinations by the judiciary related to notifications to affected individuals and/or federal agencies and related services (e.g., credit monitoring) will be made in writing by the contracting officer.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(2) No later than five business days after being directed by the contracting officer, or as otherwise required by applicable law, the contractor shall notify any individual whose PII or SPII was either under the control of the contractor or resided in an information system under control of the contractor at the time the incident occurred. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by, the contracting officer. The contractor shall not proceed with notification unless directed in writing by the contracting officer.

(3) Subject to government analysis of the incident and direction to the contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the contracting officer. Notification may require the contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(A) A brief description of the incident;

(B) A description of the types of PII or SPII involved;

(C) A statement as to whether the PII or SPII was encrypted or protected by other means;

(D) Steps individuals may take to protect themselves;

(E) What the contractor and/or the government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and

(F) Information identifying who individuals may contact for additional information.

(h) Credit Monitoring Requirements

The contracting officer may direct the contractor to:

(1) Provide notification to affected individuals, as described in paragraph (g)(2).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the contractor has no affiliation. At a minimum, credit monitoring services shall include:

(A) Triple credit bureau monitoring;

(B) Daily customer service;

(C) Alerts provided to the individual for changes and fraud; and

(D) Assistance to the individual with enrollment in the services and the use of fraud alerts.

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-57 *[cont'd]*

(3) Establish a dedicated call center. Call center services shall include:

(A) A dedicated telephone number to contact customer service within a fixed period;

(B) Information necessary for enrollees to access credit reports and credit scores;

(C) Escalation of calls that cannot be handled by call center staff, to call center management or AOUSC, as appropriate;

(D) Weekly reports on call center volume, issue escalation, and other key metrics;

(E) Customized frequently asked questions, approved in writing by the contracting officer in coordination with the Judiciary Breach Response Team (BRT); and

(F) Information for enrollees to contact customer service and fraud resolution representatives for credit monitoring assistance.

(i) Subcontracts

(1) The contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will:

(A) have access to Sensitive Information;

(B) have access to or handle systems containing Sensitive Information;

(C) collect or maintain Sensitive Information on behalf of the Judiciary; or

(D) use a subcontractor information system(s) to process, store, or transmit Sensitive Information.

(2) Any violation by a subcontractor of any of the provisions established in this clause will be attributed to the contractor.

(3) Any breach or incident, as defined in paragraph (a) (Definitions) of this clause, experienced by a subcontractor will be attributed to the contractor for the purpose of triggering contractor compliance with the requirements in paragraphs (c) (Incident Reporting Requirements), (d) (Incident Response Requirements), (f) (Other Reporting Requirements), (g) (PII and SPII Incident Notification Requirements), and (h) (Credit Monitoring Requirements) of this clause.

(end)

Clause 2-60, Stop-Work Order

Include the following clause as prescribed in § 220.25.80(d) (Service-Related Provisions and Clauses).
[. . .]

REDLINE COMPARISON REFLECTING CHANGES

Clause 2-65, Key Personnel

Include the following clause as prescribed in § 220.25.80(~~e~~d) (Service-Related Provisions and Clauses) and § 520.75(b) (Provisions and Clauses).
[. . .]

Provision 2-70, Site Visit

Include the following provision as prescribed in § 220.25.80(~~e~~f) (Service-Related Provisions and Clauses).
[. . .]

Clause 2-140, Judiciary IT Security Standards

Include the following clause as prescribed in § 220.25.80(~~f~~g) (Service-Related Provisions and Clauses).
[. . .]

Clause 3-3, Provisions, Clauses, Terms and Conditions – Small Purchases

Include the following clause as prescribed in § 310.50.30(d) (Incidental Items Not on Schedule), § 325.30.20(b) (Written Solicitations), and § 325.45.15(b) (Open Market Purchases).

Provisions, Clauses, Terms and Conditions – Small Purchases (~~OCT 2023~~JUN 2024)

[. . .]

(c) The contractor shall comply with the following clauses, incorporated by reference, unless the stated circumstances do not apply:

[. . .]

(4) Clause 2-57, Protecting, Reporting, and Responding to Incidents Involving Sensitive Information (JUN 2024) (Applies when contractor and/or subcontractor employees will have access to Sensitive Information, or have access to or handle systems containing Sensitive Information, or collect or maintain Sensitive Information on behalf of the Judiciary, or use a contractor information system(s) to process, store, or transmit Sensitive Information.)

(5) Clause 2-115, Terms for Commercial Advance Payment of Purchases (APR 2013) [. . .]

(~~5~~6) [. . .]

[Significant changes in Appendix 1C (Matrix of Solicitation Provisions and Clauses (Including Key)) follow:]

Matrix of Solicitation Provisions and Clauses *[table]*

Clause or Provision #	Title	Presc. (all references are to Volume 14)	Prov or Cls	IBR?	UCF Sec	Open Market over $100,000				T&M LH	A & E	IND DEL	SM PUR	OFAC
						FP PROD	CR PROD	FP SVC	CR SVC					
Provisions and Clauses (Chapter 2)														
2-57	Protecting, Reporting, and Responding to Incident Involving Sensitive Information	§ 220.25.80(c)	C	Yes	I	A	A	A	A	A		A	A	A
2-60	Stop-Work Order	§ 220.25.80(d)~~§ 220.25.80(c)~~	C	Yes	F	R	R	R	R	R	R	R	*	A

REDLINE COMPARISON REFLECTING CHANGES

2-65	Key Personnel (See Note 1)	§ 220.25.80(e)~~§ 220.25.80(d)~~ and § 520.75(b)	C	No	H			A	A	A		A	A	A
2-70	Site Visit	§ 220.25.80(f)~~§ 220.25.80(e)~~	P	Yes	L			A	A	A	A	A	A	
2-140	Judiciary IT Security Standards	§ 220.25.80(g)~~§ 220.25.80(f)~~	C	Yes	I	A	A	A	A	A	A	A	A	A

[Significant changes in Chapter 2 (Procurement Planning and Preparations) follow:]

§ 220 Terms and Conditions

[. . .]

§ 220.20 Warranties

[. . .]

§ 220.25.80 Service-Related Provisions and Clauses

Procurement planning also requires the CO to determine the applicability of various provisions and clauses to the performance of services. Include the following provisions and clauses as indicated:

§ 220.25.80 Service-Related Provisions and Clauses *[table]*

Clause or Provision	is included in...
(c) Clause 2-57 Protecting, Reporting, and Responding to Incidents Involving Sensitive Information	solicitations and contracts where contractor and/or subcontractor employees will: (1) have access to Sensitive Information; (2) have access to or handle systems containing Sensitive Information; (3) collect or maintain Sensitive Information on behalf of the Judiciary; or (4) use a contractor information system(s) to process, store, or transmit Sensitive Information.
(~~c~~d) Clause 2-60, Stop-Work Order	[. . .]
(~~d~~e) Clause 2-65, Key Personnel	[. . .]
(~~e~~f) Provision 2-70, Site Visit	[. . .]
(~~f~~g) Clause 2-140, Judiciary IT Security Standards	[. . .]