

# **DOD INSPECTOR GENERAL SUBPOENA REFERENCE GUIDE**



**Office of General Counsel  
Subpoena Program**

**April 2023**



## FOREWARD

A Department of Defense (DoD) Inspector General (IG) Subpoena is a valuable tool for field agents as it is often the only means of compelling the production of key records and documents during an investigation. The advantage of using a DoD IG Subpoena is that it can be used in criminal, civil, and administrative actions.

This reference guide was developed to assist field agents in the preparation of requests for DoD IG Subpoenas.

### CONTACT INFORMATION

**Mailing Address:**

Department of Defense Office of Inspector General  
ATTN: Office of General Counsel, Subpoena Program  
4800 Mark Center Drive, Suite 15K26  
Alexandria, VA 22350-1500

**E-Mail Address:** [subpoena@dodig.mil](mailto:subpoena@dodig.mil)

**Website Address:** <https://www.dodig.mil/Programs/Subpoena-Program/>

**This Reference Guide provides only internal Department of Defense Office of Inspector General guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter civil or criminal.**



## REFERENCE INDEX

| <u>SECTION</u> | <u>TOPIC</u> | <u>PAGE</u> |
|----------------|--------------|-------------|
|----------------|--------------|-------------|

### GENERAL

|      |  |    |
|------|--|----|
| 1-1  | Who Can Submit a Request for a DoD IG Subpoena                   | 7  |
| 1-2  | Benefits of Using DoD IG Subpoenas                               | 7  |
| 1-3  | Requesting a DoD IG Subpoena                                     | 8  |
| 1-4  | Methods of Serving a DoD IG Subpoena                             | 8  |
| 1-5  | DoD IG Subpoena Certificate of Return of Service                 | 8  |
| 1-6  | Request by Subpoena Recipient for Additional Time for Compliance | 9  |
| 1-7  | Delivery of Subpoenaed Records to Case Agent                     | 9  |
| 1-8  | Special Handling for Urgent / Expedited Request(s)               | 9  |
| 1-9  | Issuing Approved Subpoena Packages                               | 10 |
| 1-10 | Circumstances When a DoD IG Subpoena Would Not Be Appropriate    | 10 |

### FINANCIAL DATA

|      |  |    |
|------|--|----|
| 2-1  | Right to Financial Privacy Act (RFPA)                                | 12 |
| 2-2  | Definition of Financial Institution                                  | 12 |
| 2-3  | Definition of Financial Record                                       | 12 |
| 2-4  | Definition of Customer   | 12 |
| 2-5  | Definition of Person   | 12 |
| 2-6  | Obtaining Financial Records through a DoD IG Subpoena                | 13 |
| 2-7  | Transfer of Financial Information to another Federal Agency          | 14 |
| 2-8  | Transfer of Financial Information to Other Agencies                  | 15 |
| 2-9  | Restrictive Markings   | 16 |
| 2-10 | Obtaining Basic Identifying Bank Account Information                 | 17 |
| 2-11 | Requests for Reimbursement of Costs Associated with DoD IG Subpoenas | 17 |
| 2-12 | Handling Motions Filed to Challenge and Quash a DoD IG Subpoena      | 18 |

### ELECTRONIC DATA

|     |  |    |
|-----|--|----|
| 3-1 | Authority to Subpoena Internet/Telecom Service Providers               | 20 |
| 3-2 | Definition of Electronic Communications                                | 20 |
| 3-3 | Disclosure of Basic Subscriber Information                             | 21 |
| 3-4 | Disclosure of Other Information Pertaining to a Customer or Subscriber | 21 |



| <b><u>SECTION</u></b> | <b><u>TOPIC</u></b>   | <b><u>PAGE</u></b> |
|-----------------------|---|--------------------|
| 3-5                   | Disclosure of Electronic Communications Contents  | 22                 |
| 3-6                   | Benefits of Requesting Basic Subscriber Information from Internet / Telecom Service Providers | 23                 |
| 3-7                   | Requests for Reimbursement of Costs Associated with DoD IG Subpoenas                          | 24                 |

## **LEGAL**

|      |  |    |
|------|--|----|
| 4-1  | Legal Authority for Issuing a DoD IG Subpoena  | 26 |
| 4-2  | Unique Provisions of the IG Act Applicable to the DoD IG   | 26 |
| 4-3  | Office of General Counsel (OGC) Review of DoD IG Subpoenas   | 26 |
| 4-4  | Recipient Refusal to Comply with DoD IG Subpoena (Field Actions)   | 27 |
| 4-5  | Recipient Refusal to Comply with DoD IG Subpoena (OGC Actions)   | 28 |
| 4-6  | DoD OIG OGC Legal Review Criteria for DoD IG Subpoena  | 28 |
| 4-7  | Release of Information from Federal Travel Card Contractor   | 29 |
| 4-8  | DoD IG Subpoenas in Support of Non-Fraud Related Investigations  | 29 |
| 4-9  | DoD IG Subpoenas for Audits, Projects, and Senior Official Cases   | 30 |
| 4-10 | DoD IG Subpoenas for Educational Records   | 30 |
| 4-11 | DoD IG Subpoenas for Medical Records   | 30 |
| 4-12 | Service of a DoD IG Subpoena for Production of Documents Physically Located Outside of the United States | 35 |
| 4-13 | Requesting Additional DoD IG Subpoenas   | 35 |
| 4-14 | Service of DoD IG Subpoenas after a <i>Qui Tam</i> Case Has Been Filed                                   | 35 |

## **APPENDIXES**

|            |  |    |
|------------|--|----|
| Appendix A | Use of DoD IG Subpoenas in Support of Non-Fraud Related Investigations | 37 |
| Appendix B | Documents Required to Request DoD IG Subpoena(s)                       |    |
|            | Information Related to Agency Request Memorandum                       | 38 |
|            | Information Related to Appendix A                                      | 38 |
|            | Agency Request Memorandum Template                                     | 39 |
| Appendix C | Sample DoD IG Subpoena Packet  |    |
|            | Sample Agency Request Memorandum                                       | 43 |
|            | Sample DoD IG Subpoena Issuance Memorandum                             | 47 |
|            | Sample Custodian Letter  | 52 |
|            | Sample Subpoena <i>Duces Tecum</i>                                     | 54 |
|            | Sample Appendix A  | 56 |
|            | Basic Subscriber Information   | 57 |
|            | Financial Records (Abbreviated Version)                                | 58 |
|            | Financial Records (Expanded Version)                                   | 59 |
|            | Major Procurement Fraud Investigation                                  | 61 |



| <b><u>SECTION</u></b> | <b><u>TOPIC</u></b>   | <b><u>PAGE</u></b> |
|-----------------------|---|--------------------|
|                       | Sample Appendix B – Digital Media Specifications                                    | 69                 |
|                       | Sample Privacy Act Notice   | 83                 |
|                       | Sample Recipient Certificate of Compliance  | 85                 |
|                       | Sample Certificate of Return of Service   | 86                 |
|                       | Sample Memorandum Granting Request for Extension on DoD IG Subpoena Compliance Date | 87                 |
| Appendix D            | Instructions Concerning DoD IG Subpoenas Covered by the RFPA                        | 88                 |
| Appendix E            | Sample Packet for Financial DoD IG Subpoenas  |                    |
|                       | Sample Customer Notice Letter   | 91                 |
|                       | Sample Statement of Customer Rights   | 94                 |
|                       | Sample Instructions for Completing and Filing Motion & Sworn Statement              | 96                 |
|                       | Sample Blank Motion Form  | 97                 |
|                       | Sample Blank Statement Form (Affidavit)   | 98                 |
|                       | Sample Certificate of Service Form (Customer Notification)                          | 99                 |
|                       | Sample Agent’s Certificate of Compliance  | 100                |
| Appendix F            | Resources   | 101                |
| Appendix G            | Administrative Reminders  | 103                |
| Appendix H            | Investigative Planning Considerations   | 104                |



# GENERAL INFORMATION



| GENERAL INFORMATION |  |  |
|---------------------|--|--|
| NO.                 | TOPIC  | COMMENT  |
| 1-1                 | Who Can Submit a Request for a DoD IG Subpoena | <p>Agents of Defense Criminal Investigative Organizations (DCIOs) may request a DoD IG Subpoena. DCIOs include Defense Criminal Investigative Service (DCIS), the Department of the Army Criminal Investigation Division (CID), the Naval Criminal Investigative Service (NCIS), and the Office of Special Investigations (OSI) for the U.S. Air Force and U. S. Space Force. Other DoD investigators, law enforcement officials, and Service Inspectors General may also request a DoD IG Subpoena.</p> <p>DoD OIG components (AI, Evaluations, Audit, etc.) that require a DoD IG Subpoena should contact the DoD IG Subpoena Program Office for assistance.</p> |
| 1-2                 | Benefits of Using DoD IG Subpoenas             | <ol style="list-style-type: none"><li>1. A DoD IG Subpoena is enforceable. If the recipient fails to comply, a court order may be sought to compel compliance.</li><li>2. A DoD IG Subpoena is administrative. Unlike a grand jury subpoena, a DoD IG Subpoena can be used to support civil and administrative remedies, as well as criminal prosecutions.</li><li>3. A DoD IG Subpoena is not subject to the secrecy requirements of a grand jury subpoena.</li></ol>   |



| GENERAL INFORMATION |  |  |
|---------------------|--|--|
| NO.                 | TOPIC  | COMMENT  |
| 1-3                 | Requesting a DoD IG Subpoena                     | Transmit DoD IG Subpoena requests and supporting documentation via e-mail only to the DoD IG Subpoena Program Office at <a href="mailto:subpoena@dodig.mil">subpoena@dodig.mil</a> . When requesting multiple subpoenas for the same investigation, consolidate all recipients on one request.   |
| 1-4                 | Methods of Serving a DoD IG Subpoena             | <p>DoD IG Subpoenas should be served to the recipients by a Special Agent from the requesting DCIO and/or other military or DoD agency investigators or by registered or certified mail with a return receipt.</p> <p>In addition to agents, investigative support personnel may serve subpoenas via fax, e-mail, or law enforcement portal provided the recipient agrees, in advance, to the method of service. Confirm the method of service with the recipient to ensure it is an acceptable method of service.</p> <p>In addition to a copy of the DoD IG Subpoena and Appendixes (if applicable), the Custodian Letter addressed to the Subpoena Recipient, the Privacy Act Notice, and the Certificate of Compliance must be served upon the recipient.</p> <p>Upon receipt of a signed subpoena from the Subpoena Program Office, the subpoena should be served as soon as practicable, but no later than five business days after issuance. Requests for delays of service shall be included in the initial request for a DoD IG Subpoena.</p> |
| 1-5                 | DoD IG Subpoena Certificate of Return of Service | Complete the Certificate of Return of Service and e-mail a copy to <a href="mailto:subpoena@dodig.mil">subpoena@dodig.mil</a> IMMEDIATELY or NO LATER THAN the first business day after the subpoena is served.  |





| GENERAL INFORMATION |   |   |
|---------------------|---|---|
| NO.                 | TOPIC   | COMMENT   |
| 1-6                 | <b>Request by Subpoena Recipient for Additional Time for Compliance</b> | <p>If a recipient of a subpoena is making a good faith effort to comply with the subpoena and needs more time, a reasonable extension may be granted. Extensions do not have to be coordinated with the DoD IG Subpoena Program Office, but it is important to be cognizant of the Statute of Limitations.</p> <p>Requests for extensions to comply must be in writing. If there is reason to believe that the recipient does not intend to comply in a timely manner contact the DoD IG Subpoena Program Office. [See page 27]</p> |
| 1-7                 | <b>Delivery of Subpoenaed Records to Case Agent</b>                     | <p>The subpoena recipient can deliver the records in person, but it is acceptable to allow the recipient to mail or email the subpoenaed records.</p> <p>The method of delivery should be addressed in the subpoena cover letter and, if required, discussed with the recipient.</p> <p>Ensure that the subpoena recipient signs the Certificate of Compliance attesting that all subpoenaed documents were provided to the case agent.</p>   |
| 1-8                 | <b>Special Handling for Urgent / Expedited Request</b>                  | <p>Requests for DoD IG Subpoenas are processed in the order received by the Program Office. Approval for special handling (expedited processing) of a DoD IG Subpoena is based on Statute of Limitations considerations, the sensitivity of the investigation, and/or the impact to the investigation.</p>  |



| GENERAL INFORMATION |   |   |
|---------------------|---|---|
| NO.                 | TOPIC   | COMMENT   |
| 1-9                 | Issuing Approved Subpoena Packages                            | DoD IG Subpoenas are digitally signed by authorized Office of General Counsel (OGC) personnel and transmitted, along with associated documents, to requestor in Adobe PDF format.   |
| 1-10                | Circumstances When a DoD IG Subpoena Would Not Be Appropriate | <p>There are specific circumstances when a DoD IG Subpoena would not be appropriate or approved, unless an exception to policy is granted by OGC. These circumstances include:</p> <ul style="list-style-type: none"><li>▪ Records already in the possession of the U.S. Government;</li><li>▪ Records obtained via search warrant or grand jury subpoena;</li><li>▪ Credit Bureau information;</li><li>▪ Contents of communications;</li><li>▪ Bad check case [minimum of \$1,000 loss to the Government (DoD)];</li><li>▪ Recipient is a member of the news media (special considerations);</li><li>▪ Preliminary inquiries (subpoenas issued only for substantive cases);</li><li>▪ Records related to loss of personal property; and</li><li>▪ Recipient is an attorney and the subpoena seeks documentation regarding the attorney-client relationship.</li></ul> <p>The issuance of a DoD IG Subpoena must be in furtherance of investigations that the Inspector General considers appropriate to promote justice, maintain good order and discipline, or ensure ethical conduct throughout the DoD.</p> |



# FINANCIAL INFORMATION



| FINANCIAL INFORMATION |                                       |  |
|-----------------------|---------------------------------------|--|
| NO.                   | TOPIC                                 | COMMENT  |
| 2-1                   | Right to Financial Privacy Act (RFPA) | The Right to Financial Privacy Act (RFPA), Chapter 35, Title 12, United States Code (12 U.S.C. §§ 3401 <i>et seq.</i> ), establishes limitations, rules, and procedures for obtaining financial records from financial institutions, and sets forth penalties for Government and financial institution employees who violate the RFPA.   |
| 2-2                   | Definition of Financial Institution   | “[A]ny office of a bank, savings bank, credit card issuer as defined in section 103 of the Consumers Credit Protection Act (15 U.S.C. § 1602(o), industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution that is located in any state or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.” (12 U.S.C. § 3401) |
| 2-3                   | Definition of Financial Record        | “[A]n original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer’s relationship with the financial institution.” (12 U.S.C. § 3401)   |
| 2-4                   | Definition of Customer                | “[A]ny person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person’s name.” (12 U.S.C. § 3401)   |
| 2-5                   | Definition of Person                  | “[A]n individual or a partnership of five or fewer individuals.” (12 U.S.C. § 3401)  |



| FINANCIAL INFORMATION |   |  |
|-----------------------|---|--|
| NO.                   | TOPIC   | COMMENT  |
| 2-6                   | Obtaining Financial Records Through a DoD IG Subpoena | <p>If the subpoena is for records from a financial institution, the subpoena cannot be served until the customer notification requirements contained in the RFPA have been met.</p> <p>Serve the notification documents to the account holder and wait 10 days if you notified them in person or 14 days if you notified them via registered or certified mail with a return receipt. (The computation of days is in accordance with the Federal Rules of Civil Procedure Rule 6. If case agent wants to confirm the correct computation of days, they may contact the DoD IG Subpoena Program Office for additional assistance).</p> <p>Case Agents must check with the applicable clerks of court to determine if the account holder filed a motion to challenge. The district courts should include the Eastern District of Virginia (location of DoD OIG), the district court where the financial institution is located, and the district court where the customer resides. <b>[See Page 91]</b></p> <p>If a motion to challenge has been filed, the case agent must obtain as much information from the court clerk concerning the challenge as possible and immediately contact the DoD IG Subpoena Program Office. The subpoena may not be served upon the financial institution until the court has denied the account holder's motion.</p> <p>After the applicable clerks of court have been contacted and it has been determined that the account holder did not file a motion to challenge the subpoena, the subpoena may be served upon the financial institution along with the Certificate of Compliance attesting to compliance with the RFPA.</p> |



| FINANCIAL INFORMATION |   |  |
|-----------------------|---|--|
| NO.                   | TOPIC   | COMMENT  |
| 2-7                   | Transfer of Financial Information to Another Federal Agency | <p>Financial records may be transferred to another Federal agency or department under 12 U.S.C. § 3412 only if an official of “the transferring agency or department certifies in writing that there is [a] reason to believe the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity, investigation or analysis related to international terrorism within the jurisdiction of the receiving agency or department.”</p> <p>In addition, within 14 days of any transfer, serve or mail a copy of the certification and the following notice to the customer, at their last known address, unless the Government has obtained, in connection with its original access or at the time of the transfer, a court order delaying notice:</p> <p>Copies of, or information contained in, your financial records lawfully in possession of [name of Component] have been furnished to [name of Agency or Department] pursuant to the Right to Financial Privacy Act of 1978 [12 U.S.C. §§ 3401 <i>et seq.</i>] for the following purpose: [state the nature of the law enforcement inquiry with reasonable specificity]. If you believe that this transfer has not been made to further a legitimate law enforcement inquiry, you may have legal rights under the Right of Financial Privacy Act of 1978 or the Privacy Act of 1974 [5 U.S.C. § 552a].</p> |



| FINANCIAL INFORMATION |   |  |
|-----------------------|---|--|
| NO.                   | TOPIC   | COMMENT  |
| 2-8                   | Transfer of Financial Information to Other Agencies | Transfer restrictions do not apply to intradepartmental transfers (e.g., OSI may transfer financial records to CID or DoD litigating officers without restrictions). In addition, post-transfer notice is only required for transfers between Federal departments – the RFPA does not restrict the transfer of financial records from state or local government agencies to Federal agencies or from Federal to state and local agencies. The RFPA does not cover transfers of financial records between a Federal agency and an agency of a foreign government. The RFPA was amended in 1988, adding a provision that limits transfer of records obtained under the RFPA to the Department of Justice to only those documents relevant to violation of Federal law, and their use only for purposes for criminal investigations or prosecution purposes. The RFPA precludes the transfer of records obtained under RFPA for civil investigations other than “civil actions under section 951 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 [12 USC § 1833a], or for forfeiture under sections [section] 981 or 982 of title 18, United States Code, by the Department of Justice....” |



| FINANCIAL INFORMATION |                      |   |
|-----------------------|----------------------|---|
| NO.                   | TOPIC                | COMMENT   |
| 2-9                   | Restrictive Markings | <p>Financial records obtained via a DoD IG Subpoena should be marked with the following:</p> <p>This record was obtained pursuant to the RFPA of 1978, 12 U.S.C. §§ 3401 <i>et seq.</i>, and may not be transferred to another Federal agency or department without prior compliance with the transferring requirements of 12 U.S.C. § 3412.</p> <p>Any report of investigation or other correspondence that in its body or in its attachments contains any information obtained under the RFPA should be marked with the following restrictive legend on the front cover or first page:</p> <p>Some of the information contained herein [cite specific paragraph or attachment] is financial record information which was obtained pursuant to the RFPA of 1978, 12 U.S.C. §§ 3401 <i>et seq.</i> Do not release this information outside DoD without compliance with the specific requirements of 12 U.S.C. § 3412.</p> |





| FINANCIAL INFORMATION |   |   |
|-----------------------|---|---|
| NO.                   | TOPIC   | COMMENT   |
| 2-10                  | <b>Obtaining Basic Identifying Bank Account Information</b>                 | <p>A subpoena is required to obtain basic financial account identifying information such as name of customer, account number, addresses, and type of account.</p> <p>The request for basic financial account identifying information must be associated with either a specific financial transaction or a class of financial transactions.</p> <p>12 U.S.C. § 3413(g)</p>   |
| 2-11                  | <b>Requests for Reimbursement of Costs Associated with DoD IG Subpoenas</b> | <p>The RFPA provides for the reimbursement to financial institutions for their research and copy costs.</p> <p>Rates are established in the Code of Federal Regulations (CFR). (12 CFR 219.1 <i>et seq.</i>)</p> <p>If you receive an invoice from a financial institution requesting reimbursement for costs associated with complying with a DoD IG Subpoena, contact the DoD IG Subpoena Program Office. You should forward the invoice to the DoD IG Subpoena Program Office. The qualifying costs will be paid by the DoD OIG.</p> |



| FINANCIAL INFORMATION |   |   |
|-----------------------|---|---|
| NO.                   | TOPIC   | COMMENT   |
| 2-12                  | Handling Motions to Challenge and Quash a DoD IG Subpoena | <p>In accordance with the RFPA, the customer has a right to file a motion in a U.S. Federal District Court to quash a DoD IG Subpoena and challenge the Government's right to have access to their financial records.</p> <p>At any point during the process of obtaining financial records, if the case agent becomes aware that the customer (Subject) has filed a motion to challenge the DoD IG Subpoena under the RFPA, they must immediately notify the DoD IG Subpoena Program Office. The DoD IG Subpoena Program Office will then notify the OGC, which will then coordinate with the case agent on the preparation of an Agent Affidavit and other required documents to successfully defend the DoD OIG's interest in obtaining the customer's financial records.</p> <p>OGC has only 10 business days to prepare its rebuttal, so it is critical that the case agent work closely with the assigned OGC attorney and be responsive to any tasking from OGC on the part of the case agent.</p> |



# ELECTRONIC DATA



| ELECTRONIC DATA |   |  |
|-----------------|---|--|
| NO.             | TOPIC   | COMMENT  |
| 3-1             | Authority to Subpoena Information from Internet/Telecom Service Providers | <p>The Electronic Communication Privacy Act (ECPA), 18 U.S.C. § 2510 <i>et seq.</i> and the Stored Communications Act (SCA) 18 U.S.C. § 2701 <i>et seq.</i> establish provisions for access, use, disclosure, interception, and privacy protections of electronic communications.</p> <p>Whenever agents seek stored e-mail, account records, or subscriber information from a network service provider or telecom service provider, you must comply with the SCA.</p>   |
| 3-2             | Definition of Electronic Communications                                   | <p>According to the ECPA, 18 U.S.C. § 2510, electronic communications means, generally, “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce.” Additionally, the law establishes procedures the Government must follow in order to require a provider to disclose electronic communications.</p> <p>The ECPA and SCA prohibit an electronic communications provider from producing <u>contents</u> of electronic communications, even pursuant to subpoena or court order, except in limited circumstances.</p> |



| ELECTRONIC DATA |  |  |
|-----------------|--|--|
| NO.             | TOPIC  | COMMENT  |
| 3-3             | Disclosure of Basic Subscriber Information                             | <p>The SCA allows for the disclosure of basic subscriber information with a subpoena. This information includes:</p> <ul style="list-style-type: none"><li>▪ Name(s);</li><li>▪ Address(es);</li><li>▪ Local and long distance telephone connection records or records of session times and durations;</li><li>▪ Length of service (including start date) and types of service used;</li><li>▪ Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and</li><li>▪ Means and source of payment for such service (including any credit card or bank account number).</li></ul> <p>18 U.S.C. § 2703(c)(2)</p> |
| 3-4             | Disclosure of Other Information Pertaining to a Customer or Subscriber | <p>The SCA restricts the disclosure of records or other information pertaining to a subscriber or customer that contains transactional information. Examples of transactional information are records such as account logs that record account usage, cell-site data for cellular telephone calls, and e-mail addresses of other individuals with whom the account holder has corresponded.</p> <p>In order to obtain transactional information, a search warrant or court order is required.</p>  |



| ELECTRONIC DATA |  |   |
|-----------------|--|---|
| NO.             | TOPIC  | COMMENT   |
| 3-5             | Disclosure of Electronic Communications Contents | <p>A governmental entity seeking the contents of a wire or electronic communication from an electronic communication service provider, must obtain a search warrant or court order.</p> <p>On December 14, 2010, the Sixth Circuit decided <i>U.S. v. Warshak</i>, 631 F.3d 266. This decision had major implications for how DoD IG issues subpoenas.</p> <p>The Sixth Circuit held that the use of a 2703(d) order or subpoena (under the SCA) to compel disclosure of e-mail content from a commercial Internet Service Provider (ISP) violated the Fourth Amendment.</p> <p>The court found that people have a privacy right to the content of their e-mail, just like they do in their phone conversations or mailed letters.</p> <p>The DoD IG Subpoena Program Office will issue subpoenas for basic subscriber information.</p> |



| ELECTRONIC DATA |   |   |
|-----------------|---|---|
| NO.             | TOPIC   | COMMENT   |
| 3-5             | Disclosure of Electronic Communications Contents (Continued)                                  | <p>*If you need transactional information such as cell-site/location data, voicemails, text messages, photographs, videos, and email content, a search warrant or court order is required. The DoD IG Subpoena Program Office does not process search warrants or court orders.</p> <p>*This is not applicable to DoD or corporate e-mail and telephone communications.</p>   |
| 3-6             | Benefits of Requesting Basic Subscriber Information from Internet / Telecom Service Providers | <p>ISP Basic Subscriber Information can substantiate that the ISP customer maintained a particular ISP account and Screen ID (Facebook, Gmail, etc.). This can be of assistance, for example, when corroborating communications between a subject and victim.</p> <p>Telecom Basic Subscriber Information can provide key information such as all incoming/outgoing calls, to include blocked/restricted calls and alpha numeric text. This can be of assistance, for example, when determining a timeline of when communications occurred between the cellular phone owner and others.</p> |



| ELECTRONIC DATA |  |  |
|-----------------|--|--|
| NO.             | TOPIC  | COMMENT  |
| 3-7             | Requests for Reimbursement of Costs Associated with DoD IG Subpoenas | As with the RFPA, the SCA allows electronic communications providers to be reimbursed for research and copy costs (18 U.S.C. § 2706). Forward invoices you receive to the DoD IG Subpoena Program Office for reimbursement. Ensure you include the DoD IG Subpoena Unique Identification Number (UID) associated with the invoice. |





# LEGAL INFORMATION



| LEGAL INFORMATION |  |  |
|-------------------|--|--|
| NO.               | TOPIC  | COMMENT  |
| 4-1               | <b>Legal Authority for Issuing a DoD IG Subpoena</b>                           | The Inspector General Act of 1978 as amended. Title 5, § 406(a)(4).  |
| 4-2               | <b>Unique Provisions of the Inspector General Act Applicable to the DoD IG</b> | <p>Section 408(c) of the “Inspector General Act of 1978,” as amended, assigns the DoD Inspector General ten unique additional duties, two of which are relevant to the issues of subpoenas.</p> <p>(c)(2) Initiate, conduct, and supervise such audits and investigations in DoD (including military departments) as the IG considers appropriate.</p> <p>(c)(4) Investigate fraud, waste, and abuse uncovered as a result of other contract and internal audits, as the IG considers appropriate.</p> |
| 4-3               | <b>Office of General Counsel (OGC) Review of DoD IG Subpoenas</b>              | <p>The DoD OIG OGC reviews all requests for DoD IG Subpoenas to:</p> <ul style="list-style-type: none"><li>▪ ensure legal enforceability,</li><li>▪ ensure admissibility of evidence obtained via subpoena,</li><li>▪ help ensure the field agent gets what they need to resolve their investigation, and</li><li>▪ prevent inadvertent or intentional overreaching by the OIG or Government.</li></ul>  |



| LEGAL INFORMATION |  |  |
|-------------------|--|--|
| NO.               | TOPIC  | COMMENT  |
| 4-4               | Recipient Refusal to Comply with DoD IG Subpoena (Field Actions) | <p>If the recipient of the DoD IG Subpoena refuses to comply, immediately contact the DoD IG Subpoena Program Office. DoD OIG representatives will get additional information and coordinate with the Department of Justice (DOJ), Washington, D.C., about enforcement action. The subpoena and a request for enforcement should be sent via e-mail to the DoD IG Subpoena Program Office with a copy to the DoD OIG OGC. The designated OGC attorney will assist the field agent in preparing an affidavit to be filed in a District Court proceeding.</p> <p>The case agent should be prepared to provide the following information:</p> <ul style="list-style-type: none"><li>▪ detailed information outlining noncompliance, lack of compliance, or partial compliance; copies of subpoena, proof of service, and memorandum requesting subpoena;</li><li>▪ copies of all correspondence related to subpoena compliance and/or notes of telephone conversations and e-mail communications;</li><li>▪ synopsis detailing efforts to obtain compliance; i.e., telephone calls, discussions, extensions granted; and</li><li>▪ synopsis of investigative efforts to date.</li></ul> |



| LEGAL INFORMATION |  |   |
|-------------------|--|---|
| NO.               | TOPIC  | COMMENT   |
| 4-5               | Recipient Refusal to Comply with DoD IG Subpoena (OGC Actions) | <p>If the recipient of a DoD IG Subpoena refuses to comply, immediately contact the DoD IG Subpoena Program Office. DoD OIG representatives will get additional information and coordinate with DOJ about enforcement action.</p> <p>The DoD OIG OGC will take the following enforcement action steps:</p> <ul style="list-style-type: none"><li>▪ may attempt to obtain compliance without DOJ action,</li><li>▪ if unable to obtain compliance, will work with field agent to prepare enforcement package for DOJ, and</li><li>▪ after DoD IG concurrence, will forward enforcement package to DOJ/USAO for action.</li></ul> |
| 4-6               | DoD OIG OGC Legal Review Criteria for DoD IG Subpoena          | <p>The DoD OIG OGC subpoena review criteria are:</p> <p><b>Legal Standards</b></p> <ul style="list-style-type: none"><li>▪ Is it within the authority of the DoD OIG?</li><li>▪ Is the demand reasonably relevant to the subject matter of the investigation?</li><li>▪ Is the demand overly broad or unduly burdensome?</li></ul>  |



| LEGAL INFORMATION |   |   |
|-------------------|---|---|
| NO.               | TOPIC   | COMMENT   |
| 4-6               | DoD OIG OGC Legal Review Criteria for DoD IG Subpoena (Continued) | <b>Additional Factor</b> <ul style="list-style-type: none"><li>▪ Is the subpoena addressed properly, i.e., custodian of records?</li><li>▪ Are company and individual names consistent and spelled correctly?</li><li>▪ Is the address correct and consistent?</li><li>▪ Is the location of return of service consistent and correct?</li><li>▪ Is the DoD nexus clear?</li></ul>                             |
| 4-7               | Release of Information from Federal Travel Card Contractor        | 12 U.S.C. § 3413(q), “Exceptions,” “Disclosure of information with respect to a Federal contractor-issued travel charge card.”<br>“Nothing in this title [i.e., the Right to Financial Privacy Act] shall apply to the disclosure of any financial record or information to a Government authority in conjunction with a Federal contractor-issued travel charge card issued for official Government travel.” |
| 4-8               | DoD IG Subpoenas in Support of Non-Fraud Related Investigations   | Subpoenas can be requested for non-fraud-related investigations that satisfy the DoD nexus test criteria. The Defense Criminal Investigative Organization (DCIO) submitting the request must have investigative authority for the crime(s) under investigation and the particular crime at issue must be of such a nature and/or concern to DoD as to warrant the DoD OIG’s involvement in the investigation. |



| LEGAL INFORMATION |  |   |
|-------------------|--|---|
| NO.               | TOPIC  | COMMENT   |
| 4-9               | DoD IG Subpoenas for Audits, Projects, and Senior Official Cases | <p>DoD IG Subpoenas issued in support of audit, special projects, senior official investigations, and other DoD OIG internal components, must meet the following criteria:</p> <ul style="list-style-type: none"><li>▪ must have a clear DoD nexus,</li><li>▪ U.S. Government does not already possess the records or have other means of obtaining the records,</li><li>▪ records are relevant to ascertaining the truth in the matter,</li><li>▪ request not unduly broad or burdensome, and</li><li>▪ reasonable alternatives have been unsuccessful or are impracticable.</li></ul> |
| 4-10              | DoD IG Subpoenas for Educational Records                         | <p>As per the Family Educational Rights and Privacy Act (FERPA) (20 USC § 1232g), educational institutions may lose Federal funding if they permit the release of records without a parent's written consent. However, subpoenas issued for "law enforcement purposes" are an exception. The issuing agency may also order nondisclosure of notification by institution employees.</p> <p>20 U.S.C. § 1232g(b)(1)(J)(ii); 34 CFR Part 99</p>  |
| 4-11              | DoD IG Subpoenas for Medical Records                             | <p><b>Standard Medical Records</b></p> <p>A covered entity* may disclose protected health information for a law enforcement purpose if the administrative subpoena requests information and/or documents which meet the following criteria:</p>   |



| LEGAL INFORMATION |  |   |
|-------------------|--|---|
| NO.               | TOPIC  | COMMENT   |
| 4-11              | DoD IG Subpoenas for Medical Records (Continued) | <p><b>Standard Medical Records (Continued)</b></p> <p>a. “The information sought is relevant and material to a legitimate law enforcement inquiry [(i.e., the investigation of a DoD healthcare provider suspected of defrauding the DoD)];</p> <p>b. “The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and</p> <p>c. De-identified information could not reasonably be used.”</p> <p>45 CFR § 164.512(f)(1)(ii)(C)</p> <p>* Covered entity means (45 CFR § 160.103):</p> <p>(1) “A health plan.</p> <p>(2) A health care clearinghouse.</p> <p>(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”</p> <p><b>Psychotherapy Medical Records</b></p> <p>45 CFR § 164.508, “Uses and disclosures for which an authorization is required.”</p> <p>(a) “Standard: Authorizations for uses and disclosures –</p> <p>(1) Authorization required: General rule.</p> <p>Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.</p> |



| LEGAL INFORMATION |  |  |
|-------------------|--|--|
| NO.               | TOPIC  | COMMENT  |
| 4-11              | DoD IG Subpoenas for Medical Records (Continued) | <p><b>Psychotherapy Medical Records (Continued)</b></p> <p>When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization..</p> <p>(2) Authorization required: Psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:</p> <p>(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).”</p> <p>45 CFR § 164.512, “Uses and disclosures for which an authorization or opportunity to agree or object is not required.”</p> <p>“A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section.</p> |





| LEGAL INFORMATION |  |  |
|-------------------|--|--|
| NO.               | TOPIC  | COMMENT  |
| 4-11              | DoD IG Subpoenas for Medical Records (Continued) | <p><b>Psychotherapy Medical Records (Continued)</b></p> <p>When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.</p> <p>(a) Standard: Uses and disclosures required by law.</p> <p>(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.</p> <p>(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law."</p> <p>"(f) Standard: Disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.</p> |



| LEGAL INFORMATION |  |   |
|-------------------|--|---|
| NO.               | TOPIC  | COMMENT   |
| 4-11              | DoD IG Subpoenas for Medical Records (Continued) | <p><b>Psychotherapy Medical Records (Continued)</b></p> <p>(1) Permitted disclosures: Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:</p> <p>(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or</p> <p>(ii) In compliance with and as limited by the relevant requirements of:</p> <p>(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;</p> <p>(B) A grand jury subpoena; or</p> <p>(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:</p> <p>(1) The information sought is relevant and material to a legitimate law enforcement inquiry;</p> <p>(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and</p> <p>(3) De-identified information could not reasonably be used.”</p> |



| LEGAL INFORMATION |  |   |
|-------------------|--|---|
| NO.               | TOPIC  | COMMENT   |
| 4-12              | Service of a DoD IG Subpoena for Production of Documents Physically Located Outside of the United States | The IG Act contains no provisions for service of process extraterritorially (i.e., outside the United States). You must serve the subpoena to someone in the U.S. (corporate agent representative, or subsidiary), so that the DoD OIG is able to obtain jurisdiction over the party with records in any necessary enforcement proceeding to obtain the records.  |
| 4-13              | Requesting Additional DoD IG Subpoenas   | Additional subpoenas may be requested on a matter where a DoD IG Subpoena has been previously issued. The additional subpoena cannot request the identical documents/records, but it can cover a different time period, contract, or documents not previously requested.  |
| 4-14              | Service of DoD IG Subpoenas After a <i>Qui Tam</i> Case Has Been Filed                                   | <p>A DoD IG Subpoena may be served after a <i>qui tam</i> case has been filed because the Government is not a party to a <i>qui tam</i> case until it formally intervenes in the case.</p> <p>(31 U.S.C. § 3730)</p> <p>Once the DOJ and/or the USAO intervenes in a <i>qui tam</i> suit, use of a DoD IG Subpoena could be viewed as improper by the trial court and result in sanctions against the DOJ attorney/AUSA and/or dismissal of the case.</p> |



# APPENDIXES



## APPENDIX A - USE OF DOD IG SUBPOENAS IN SUPPORT OF NON-FRAUD RELATED INVESTIGATIONS



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500

MAY 23 2018


MEMORANDUM FOR DIRECTOR, DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
COMMANDER, UNITED STATES ARMY CRIMINAL  
INVESTIGATION COMMAND  
DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE  
COMMANDER, AIR FORCE OFFICE OF SPECIAL  
INVESTIGATIONS

SUBJECT: Use of Department of Defense Inspector General (DoD IG) Subpoenas in Support of  
Non-Fraud Related Investigations

Reference: Department of Defense Inspector General Memorandum, "Use of DoD IG Subpoenas in  
Support of Non-Fraud Related Investigations," June 16, 2009

This memorandum cancels the reference, which required an exception to policy for the issuance of DoD Office of Inspector General Subpoenas, in support of certain non-fraud related criminal investigations conducted by the Defense Criminal Investigative Organizations (DCIOs). The DoD OIG will continue to issue Inspector General Subpoenas in support of non-fraud related investigations conducted by the DCIOs and other DoD Components, in accordance with DoD Instruction 5505.16, "Investigations by DoD Components." Exceptions to policy will no longer be required for non-fraud related investigations. For the DoD OIG to issue a non-fraud related subpoena, the DoD Component submitting the request must have investigative authority for the matter(s) under investigation, the investigation must have a clear DoD nexus, and the subpoena demand must be relevant to the subject matter of the investigation. Finally, issuance of the subpoena must be in furtherance of investigations that the Inspector General considers appropriate to promote justice, maintain good order and discipline, or ensure ethical conduct throughout DoD.

[REDACTED]

  
Glenn A. Fine  
Principal Deputy Inspector General  
Performing the Duties of the Inspector General



## APPENDIX B – DOCUMENTS REQUIRED TO REQUEST DOD IG SUBPOENA(S)

### AGENCY REQUEST MEMORANDUM

This memorandum, prepared on agency letterhead, contains 20 interrogatories that provide information about the investigation and documents requested. It provides information that is vital to determining if the request meets the DoD IG's statutory authority, if documents are relevant to the investigation, and that the request is not overly broad or unreasonably burdensome.

Agency Request Memorandums must be reviewed by a supervisor; however, a signature is not required.

The first time an acronym appears, establish it by spelling out the full term or name, then provide the acronym in parentheses.

If requesting multiple subpoenas for the same investigation, requestor only needs to complete/submit one Agency Request Memorandum containing all the required information.

All Agency Request Memorandums must be submitted in Microsoft Word® format in the event it must be edited and/or information needs to be copied and pasted in preparation of supporting documents generated by the DoD IG Subpoena Program Office.

### APPENDIX A

The Appendix A, if needed, describes the records being subpoenaed. The Appendix A may not compel the creation of list or documents not already in existence.

The Appendix A, if needed, is prepared by the DoD IG Subpoena Program Office except for major procurement fraud cases wherein documents are being subpoenaed from a Contractor/Subcontractor.

When not required to submit an Appendix A, the requestor must described the records being requested in Block 20 of the Agency Request Memorandum. If subpoena recipient is an Internet Service Provider (ISP), Telecom/Cellular Carrier, and Social Media Platform, requestor may annotate "Basic subscriber information from [identified subpoena recipient] associated with [targeted phone number, email address, IP address]."

If requesting documents from a Contractor/Subcontractor associated with a procurement fraud investigation, requestor is required to submit an Appendix A in Microsoft Word® format in the event it must be edited. If request is in support of a civil procurement fraud investigation, an Appendix B (Specification of ESI and Digitized ("Scanned") Images ("Production Specifications")) may be required. If the supporting legal counsel requires a specific version of the Specification of ESI, please provide to the DoD IG Subpoena Program Office at the time of request.



**(Agency Letterhead)**

**MEMORANDUM FOR SUBPOENA PROGRAM DIRECTOR, OFFICE OF GENERAL COUNSEL, OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF DEFENSE**

**SUBJECT: Request for DoD IG Subpoena(s)**

**1. Requesting Agent/Investigator:**

- a. Name: **[Enter title and name here]**
- b. Office and mobile phone numbers: **[Enter your office and mobile phone numbers here. If you are located overseas, please provide a DSN also.]**
- c. Email address: **[Enter your work e-mail address here]**
- d. Organization and street address: **[Enter your work agency and address here, to include your zip code]**
- e. Have you received training from the DoD IG Subpoena Team? **[Yes or No]**

**2. Reviewing Supervisor:**

- a. Name: **[Enter supervisor's name here]**
- b. Title: **[Enter supervisor's title here]**
- c. Office and mobile phone numbers: **[Enter supervisor's office and mobile phone numbers here.]**
- d. Email address: **[Enter supervisor's work e-mail address here]**
- e. Date of Approval: **[Enter date supervisor reviewed and approved request here]**

**3. Case file number (Full LER/ROI Number): [Enter your full case number here]**

**4. Is this a substantive investigation? [Enter whether your investigation is a substantive investigation here – DoD IG Subpoenas are not issued for developmental investigations or preliminary inquiries.]**

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



5. List investigative agencies participating jointly in this investigation and identify which agency is the lead agency: **[Enter all agencies (spell out acronyms) participating in the investigation and designated lead (if applicable) agency here]**

6. Have DoD IG Subpoenas been issued previously in this investigation? If so, please provide the DoD IG Subpoena UID Number and identity of the recipient. **[Enter yes or no and if applicable, enter the DoD IG Subpoena UID Number and identity of recipient here]**

7. Statute(s) and/or UCMJ article(s) believed to be violated: (Provide the full UCMJ or U.S.C. Section and Title, i.e., UCMJ Article 132, Fraud against the U.S. Government.) **[Enter the appropriate UCMJ Article(s) and/or Federal/State Criminal Statutes here - this should match what is listed on your LER. There may not be a UCMJ Article or criminal statute for death investigations. You may list Undetermined Death.]**

8. Subject(s) of the investigation:

a. Rank/Title and Full Name or Company Name: **[Enter Subject's Rank/Title and name or company name here]**

b. Status (i.e. active duty, reserve, dependents, civilian, contractor, etc.): **[Enter Subject's Status or N/A here]**

c. Unit/Agency or Company Address: **[Enter Subject's unit info or company address here]**

9. Summary of information to include source of initial information; sufficient details to understand the who, what, when, where, and how it pertains to the violation of the statutes and/or UCMJ punitive articles identified above; how the requested records are relevant to your investigation; and the DoD nexus: **[Enter a detailed summary of who, what, when, where, why, and how of the investigation here. Provide detailed summary of the crime and investigative efforts. Let the summary flow chronologically. Typically, you can use your write-up from your Initial/Status Report and then add a little more information to it to show how the records you are requesting came about and how they are relevant to your investigation.]**

**Need to provide, at a minimum, (1) an explanation of the workings of the incident being investigated, (2) a chronological summary of the investigative information gathered to date, and (3) an explanation of why the documents/categories of documents being requested are relevant to the investigation (i.e. how will the requested documents/categories of documents assist in proving the elements of the offense(s) identified above). It is critical to provide this information in order for the Subpoena Program to make a determination as to whether the request meets the criteria for approval. We do not need all your investigative activity that you have conducted - only what is needed to support your subpoena request.]**

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**





10. Legal Coordination:

- a. Name: **[Enter the rank (if applicable) and name of the AUSA, SAUSA, DOJ trial attorney, or military trial counsel who you coordinated with regarding this request.]**
- b. Title: **[Enter legal counsel's title here]**
- c. Office and mobile phone numbers: **[Enter legal counsel's office and mobile phone numbers here.]**
- d. Email address: **[Enter legal counsel's work e-mail address here]**
- e. Date of Concurrence (The coordination is not to obtain a legal opine or prosecutorial decision. It is to determine if they concur and support the request for a DoD IG Subpoena.): **[Enter date legal counsel reviewed and concurred with this request here]**

11. Date range of requested records sought (specify the beginning and ending dates): **[Enter the time period (month/day/year) for the requested records here]**

12. Relevancy of the date range requested: **[Enter why the listed time period is relevant to your investigation here]**

13. If the case pertains to a contract, which organization was the contracting authority, what is (are) the contract number(s), what is (are) the period(s) of performance, and what goods or services are/were procured? **[Enter the contract information if the case pertains to a contract here]**

14. Provide the legal name(s) and physical street address of the subpoena recipient(s): (Post Office boxes are not typically acceptable.) **[Enter the full legal name(s) of the subpoena recipient(s) and/or who the subpoena should be directed to and their full mailing address (to include zip code) here]**

**\*\* Subpoena request for multiple recipients for the same investigation should be consolidated into one subpoena request memorandum. \*\***

15. Is the subpoena recipient for financial (i.e. bank, credit union, savings and loan, or credit card issuer); educational, employment, or medical records? If so, provide the following information:

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



- a. Financial Records ONLY – account holder’s full name, mailing address (If Subject is deceased, provide the name and mailing address of the Next of Kin/Executor of the deceased's estate.), and targeted account number(s): **[If applicable, enter the full name of the account holder, their mailing address, and the targeted account number here]**
- b. Financial, Educational, Employment, and Medical Records ONLY – Last four of SSN: **[If applicable, enter the last four of the individual’s SSN you are requesting records for here]**
- c. Educational, Employment, and Medical Records ONLY – Date of Birth: **[If applicable, enter the individual you are requesting records for Date of Birth here]**

16. Are the records sought already in the possession of a Federal government agency? If yes, identify the Federal agency and the rationale for issuing a subpoena for records we (the government) already have. **[If applicable, enter identification of the agency and rationale for requesting records already in the possession of a federal agency here]**

17. Have the records sought already been obtained through a search warrant or grand jury subpoena? If yes, explain. **[If applicable, enter information concerning records already sought via a grand jury or search warrant here]**

18. How will the records sought assist in this investigation? **[Enter detailed information on what you expect the records to reflect and/or how they are going to assist/support your investigation here]**

19. Include any other information you believe is important. **[Enter any information that you believe needs to be further explained and/or highlighted here to assist our office during our investigative/legal sufficiency review]**

20. Individually describe the records, or classes of records you require (subpoena appendix items). **[Enter a detailed description or list of records, documents, etc. that you are requesting from the subpoena recipient here]**

**\* If you have a separate Appendix A, you may state “See Attached Appendix A.” \***

**\*\* Once you have completed your request, submit it to [subpoena@dodig.mil](mailto:subpoena@dodig.mil) in Word format and do not forget to change the letterhead to your office's letterhead. When requesting multiple subpoenas for the same investigation, you only need to complete/submit one request containing all the required information. Please feel free to contact the DoD IG Subpoena Team if you have any questions. \*\***

**\*\*\* You may request a template in Word version by sending an email to [subpoena@dodig.mil](mailto:subpoena@dodig.mil). \*\*\***

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



## APPENDIX C – DOD IG SUBPOENA SAMPLE PACKAGE

### AGENCY REQUEST MEMORANDUM

See Appendix B for a detailed explanation regarding the Agency Request Memorandum.

#### (Agency Letterhead)

#### MEMORANDUM FOR SUBPOENA PROGRAM DIRECTOR, OFFICE OF GENERAL COUNSEL, OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Request for DoD IG Subpoena(s)

1. Requesting Agent/Investigator:

- a. Name: **Special Agent Harvey Specter**
- b. Office commercial phone number and cellular phone number: **(703) 604-xxxx (office); (202) 330-xxxx (cellular)**
- c. Email address: **harvey.specter@us.army.mil**
- d. Organization and street address: **Maryland Fraud Resident Agency, 5115 Pistol Road, Aberdeen Proving Ground, Maryland 21005**
- e. Have you received training from the DoD IG Subpoena Team? **Yes**

2. Reviewing Supervisor:

- a. Name: **Special Agent John Q. Doe**
- b. Title: **Resident Agent-in-Charge**
- c. Office commercial phone number and cellular phone number: **(703) 604-xxxx (office); (703) 604-xxxx (cellular)**
- d. Email address: **john.q.doe.mil@mail.mil**
- e. Date of Approval: **March 29, 2023**

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



3. Case file number (Full LER/ROI Number): **0000-2021-CID000-000**

4. Is this a substantive investigation? (DoD IG Subpoenas are not issued for developmental investigations or preliminary inquiries.) **Yes. This is a substantive investigation.**

5. List investigative agencies participating jointly in this investigation and identify which agency is the lead agency:

**CID, Major Procurement Fraud Unit (Lead)**  
**Defense Criminal Investigative Service**  
**Air Force Office of Special Investigations**  
**Naval Criminal Investigative Service**

6. Have DoD IG Subpoenas been issued previously in this investigation? If so, please provide the DoD IG Subpoena UID Number and identity of the recipient. **Yes.**

**DoD IG Subpoena 2023XXXX-XXXXX (ABC Co.)**

7. Statute(s) or UCMJ article(s) believed to be violated: (Provide the full UCMJ or U.S.C. Section and Title, i.e., UCMJ Article 132, Fraud against the U.S. Government.) **UCMJ Article 121, Larceny and 18 U.S.C. § 287, False Claims**

8. Subject(s) of the investigation:

a. Rank/Title and Full Name or Company Name: **ACE International, Inc.**

b. Status (i.e. active duty, reserve, civilian, etc.): **Department of Defense (DoD) Contractor**

c. Unit/Agency or Company Address: **ACE International Inc., 123 Main Street, Anytown, Anystate 12345**

9. Brief summary of information to include the source of initial information. Provide details sufficient enough to understand the who, what, when, where, and how as it pertains to the violation of the statutes and/or UCMJ punitive articles identified above; how the requested records are relevant to your investigation; and the DoD nexus.: **This investigation was initiated based on information received from ...**

**On 15 Jun 03, the U.S. Army Soldier and Biological Chemical Command (SBCCOM), now the Research Development and Engineering Command (RDECOM), awarded ACE International, Inc. (ACE) an indefinite quantity/indefinite delivery contract with time and materials task orders for environmental sciences support, contract number ACE-15-A-1234, with a five year performance period, valued at \$20,000,000.00. ACE subsequently subcontracted a portion of the work to Tri Work.**

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



**Witness alleged ACE made false claims by billing the government for labor categories their employees were not qualified for under the terms of the contract. The amount or percentage of the labor mischarging has not yet been determined.**

10. Legal Coordination:

- a. Name: **AUSA Bob Smith**
- b. Title: **AUSA**
- c. Office and mobile phone numbers: **(301) 555-xxxx (Office); (301) 555-xxxx (Cell)**
- d. Email address: **bob.smith@ausa.office.gov**
- e. Date of Concurrence (The coordination is not to obtain a legal opine or prosecutorial decision. It is to determine if they concur and support the request for a DoD IG Subpoena.): **March 28, 2023**

11. Date range of requested records sought (specify the beginning and ending dates): **15 Jun 15 through 14 Jun 20**

12. Relevancy of the date range requested: **ACE has submitted numerous invoices to the government, which paid about \$2.4 million for those invoices during the contract period of performance of 15 Jun 15 to 14 Jun 20.**

13. If the case pertains to a contract, which organization was the contracting authority, what is (are) the contract number(s), what is (are) the period(s) of performance, and what goods or services are/were procured? **Ms. Jane Jones, Contracting Officer, Robert Ames Acquisition Center – Edgewood Branch, APG, MD 22232; U.S. Army Contract Number: ACE-15-A-1234; Period of Performance: 15 Jun 15 through 14 Jun 20; Environmental Services Support**

14. Provide the legal name(s) and physical street address of the subpoena recipient(s): (Post Office boxes are not acceptable.) **ACE International, Incorporated, ATTN: Legal Processing, 123 Main Street, Anytown, Anystate 12345**

15. Is the subpoena recipient for financial (i.e. bank, credit union, savings and loan, or credit card issuer); educational, employment, or medical records? If so, provide the following information:

- a. Financial Records ONLY – account holder’s full name, mailing address (If Subject is deceased, provide the name and mailing address of the Next of Kin/Executor of the deceased’s estate.), and targeted account number(s): **N/A**

**CONTROLLED UNCLASSIFIED INFORMATION / LAW ENFORCEMENT SENSITIVE**



b. Financial, Educational, Employment, and Medical Records ONLY – Last four of SSN: N/A

c. Educational, Employment, and Medical Records ONLY – Date of Birth: N/A

16. Are the records sought already in the possession of a Federal government agency? If yes, identify the Federal agency and the rationale for issuing a subpoena for records we (the government) already have. **No.**

17. Have the records sought already been obtained through a search warrant or grand jury subpoena? If yes, explain. **No**

18. How will the records sought assist in this investigation? **The records will show which employees were billed against which labor categories as well as the employee's qualifications. This will quantify the over-billed amount.**

19. Include any other information you believe is important. **None.**

20. Individually describe the records, or classes of records you require (subpoena appendix items). **Certified payroll documents pertaining to all invoices submitted under contract ACE-15-A-1234; complete resumes for all employees who have had hours billed to contract ACE-15-A-1234; all documents used to substantiate labor hours and labor categories on invoices submitted under contract ACE-15-A-1234.**



### **DOD INSPECTOR GENERAL SUBPOENA ISSUANCE MEMORANDUM**

This memorandum provides information on how to serve a DoD IG Subpoena, including what documents to serve; information regarding DoD IG Subpoenas for financial institutions and RFPA requirements; and additional actions required by the requestor after the subpoena has been served.

If requestor has any questions after reviewing the DoD Inspector General Subpoena Issuance Memorandum, please contact the specified Agent/Senior Investigator on the DoD IG Subpoena Program Team identified in the issuance email. Contact information for the DoD IG Subpoena Program Office is provided in the DoD Inspector General Subpoena Issuance Memorandum.

## **Guidance on DoD Inspector General Subpoena Issuance Memorandum**

**FROM: DoD Inspector General Subpoena Program Office**

**SUBJECT: Guidance on DoD Inspector General Subpoena Issuance**

**In the attached Adobe documents, you will find your digitally signed and issued DoD Inspector General (IG) Subpoena(s), with the appropriate associated documents.**

**We would like to take this time to review several key elements associated with your recently issued DoD IG Subpoena.**

### **1. SERVICE OF THE SUBPOENA**

**Serve a copy of the Custodian Letter, digitally signed DoD IG Subpoena, Appendix/Appendices (as applicable), Privacy Act Statement, and Certificate of Compliance to the intended recipient (entity or individual reflected on the face of the subpoena) as soon as practicable but NO LATER THAN five business days unless otherwise coordinated with the Subpoena Program Office.**

**After the subpoena is served on the recipient, complete and return the Certificate of Return of Service IMMEDIATELY or as soon as practicable to the DoD IG Subpoena Program Office at [subpoena@dodig.mil](mailto:subpoena@dodig.mil). The Certificate of Return of Service is to be completed by the serving Agent/Investigator at the time the subpoena is served. This lets our office know you have served the subpoena. It does not pertain to the return of documents.**

**You may serve the subpoena in person or by registered or certified mail with a return receipt. The subpoena can also be served via fax or email providing the recipient agrees in advance or through the recipient's established online portal.**



DoD IG Subpoenas can only be served to the recipients by a Special Agent from the requesting Defense Criminal Investigative Organization (DCIO) and/or other military or DoD agency investigators.

If the subpoena is for records from a financial institution, you must follow the requirements listed in the section below.

## **2. RIGHT TO FINANCIAL PRIVACY ACT (RFPA) REQUIREMENTS**

The RFPA (hereafter, the “Act”) affects subpoenas served on a “financial institution” for records concerning a “customer” of that financial institution as defined by the Act. “Financial institution” includes traditional banks and savings and loan institutions, credit unions, and credit card issuing institutions. Investment firms, for example, would not be financial institutions under the Act unless they issue credit cards or offer draft accounts. “Customer” includes an individual or a partnership of five or fewer partners. Larger partnerships and corporations (regardless of the number of corporate owners) are not “customers” under the Act.

The purpose of the Act is to provide added privacy to a customer’s financial records. Concerning subpoenas for financial records, the Act requires that a customer be notified of the Government’s intention to obtain financial records prior to the actual service of a subpoena. Upon receiving such notification, then, a customer may file a motion in Federal district court to challenge the subpoena. To prevail, the customer must be able to show that the records sought are either not relevant to your investigation, are unduly broad in scope, or that the investigation itself is either unauthorized or baseless. Accordingly, most challenges are unsuccessful because subpoena requests are screened for the same attributes before they are approved.

If your subpoena is for basic identifying account information associated with an account held by a financial institution, the Act does not apply. If your subpoena is for financial records for larger partnerships and corporations (regardless of the number of corporate owners), the Act does not apply. If your subpoena is for a customer’s financial records, you cannot serve the subpoena until you have met the RFPA requirements.

### **Process for Serving DoD IG Subpoenas on Financial Institutions:**

- a. Serve the notification documents [RFPA Customer Notice, copy of Subpoena Duces Tecum and any Appendices, Statement of Customer Rights under the RFPA, Instructions for Completing and Filing Motion and Sworn Statement, Motion Form, Sworn Statement Form, and Certificate of Service] to the account holder/customer.
- b. Wait at least 10 business days if you notified them in person or at least 14 business days if you notified them via registered or certified mail with a return receipt.





For the purpose of this customer notice, time is calculated in accordance with Rule 6 of the Federal Rules of Civil Procedure; i.e., (a) the day the notice is provided is excluded, (b) exclude intermediate Saturdays, Sundays, and legal holidays when the period is less than 11 days, (c) include the last day of the period unless it is a Saturday, Sunday, legal holiday or – if the act to be done is filing a paper in court – a day on which weather or other conditions make the clerk’s office inaccessible; when the last day is excluded, the period runs until the end of the next day that is not a Saturday, Sunday, legal holiday or a day on which weather or other conditions make the clerk’s office inaccessible.

The Customer Notice instructs the account holder to serve the Government authority requesting the records by mailing (by registered or certified mail) or by delivering a copy of your motion and sworn statement to: Inspector General of the Department of Defense, c/o DoD IG Subpoena Program Manager, 4800 Mark Center Drive, Suite 11H25, West Tower, Alexandria, VA 22350-1500.

c. Contact the applicable Clerks of Court offices (Eastern District Court of Virginia, district court where account holder/customer resides, and district court of where the financial institution is located) to determine if the account holder/customer has filed a motion to challenge the subpoena.

If the DoD IG Subpoena Program Office receives notice that a challenge was filed, we will immediately notify you and turn the matter over to our Office of General Counsel (OGC) for review and action. Regardless of whether or not the account holder sent you or the DoD IG Subpoena Program Office a certificate of service, you must still check with the applicable clerks of court to determine if the account holder filed a motion to challenge the subpoena.

If for some reason the account holder filed a motion to challenge the subpoena and notifies you instead of us, please contact the DoD IG Subpoena Program Office immediately.

If after you have contacted the applicable clerks of court and determined the account holder did not file a motion to challenge the subpoena, you may then serve the financial institution the Custodian Letter, digitally signed DoD IG Subpoena, Appendix/Appendices (as applicable), Privacy Act Notice, Certificate of Compliance, and the Agent’s RFPA Certificate of Compliance certifying that you have complied with all RFPA requirements.

### **Restrictive Markings**

Financial records obtained via a DoD IG Subpoena should be marked with the following: “This record was obtained pursuant to the RFPA of 1978, 12 U.S.C. 3401 et seq., and may not be transferred to another Federal agency or department without prior compliance with the transferring requirements of 12 U.S.C. 3412.”



Any report of investigation or other correspondence that in its body or in its attachments contains any information obtained under the RFPA should be marked with the following restrictive legend on the front cover or first page: “Some of the information contained herein [cite specific paragraph or attachment] is financial record information which was obtained pursuant to the RFPA of 1978, 12 U.S.C. 3401 et seq. Do not release this information outside DoD without compliance with the specific requirements of 12 U.S.C. 3412.”

#### **Transfer of Financial Information Obtained via DoD IG Subpoena to Other Agencies**

Financial records may be transferred to another Federal agency under 12 U.S.C. 3412 only if an official of the transferring agency certifies in writing that there is a reason to believe the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity (to include investigation or analyses related to international terrorism) within the jurisdiction of the receiving agency. In addition, within 14 days after any transfer, serve or mail to the customer, at his or her last known address, unless the Government has obtained, in connection with its original access or at the time of the transfer, a court order delaying notice, the following notice: “Copies of or information contained in your financial records lawfully in possession of [name of Component] have been furnished to [name of Agency or Department] pursuant to the Right to Financial Privacy Act of 1978 for the following purposes: [state the nature of the law enforcement inquiry with reasonable specificity]. If you believe that this transfer has not been made to further a legitimate law enforcement inquiry, you may have legal rights under the Right of Financial Privacy Act of 1978 or the Privacy Act of 1974.”

If a request for release of information is from a Federal Agency authorized to conduct foreign intelligence or foreign counterintelligence activities, the information shall be released without notifying the customer, unless permission to provide notification is given in writing by the requesting Agency.

Transfer restrictions do not apply to intradepartmental transfers (e.g., OSI may transfer financial records to CID or DoD litigating officers without restrictions). In addition, post-transfer notice is only required for transfers between Federal departments – the RFPA does not restrict transfer of financial records from state or local government agencies to Federal agencies or from Federal to state and local agencies. Neither does the RFPA cover transfers of financial records between a Federal agency and an agency of a foreign government. The RFPA was amended in 1988, adding a provision that limits transfer of records obtained under the RFPA to the Department of Justice to only those documents relevant to violation of Federal criminal law, and their use only for criminal investigative or prosecutive purposes.

Under the RFPA, financial institutions are entitled to reimbursement of expenses such as labor, reproduction costs, etc. In the event you receive a request for reimbursement of expenses from the respective financial institution, please forward the invoice or request for payment to our office at [subpoena@dodig.mil](mailto:subpoena@dodig.mil).



### **3. FOLLOW-UP REPORTS**

Once a DoD IG Subpoena is issued, the case falls under the oversight of the DoD IG; however, we no longer require DCIOs to provide Final Reports of Investigation (ROI)/Law Enforcement Reports (LER) without attachments once the case is closed and all action is taken. In the event our leadership request information for a specific investigation supported by a DoD IG Subpoena, the DoD IG Subpoena Program Office will contact and coordinate the matter with the respective case agent and their supervisor.

### **4. ENCOUNTERING DIFFICULTIES WITH THE SUBPOENA SERVICE**

Contact the DoD IG Subpoena Program Office if you encounter difficulties with the subpoena process or service that may be remedied with our assistance.

### **5. CONTACT INFORMATION**

**Mailing Address:**

**Inspector General, Department of Defense  
Office of General Counsel, General Counsel Investigations  
ATTN: DoD IG Subpoena Program Office  
4800 Mark Center Drive, Suite 11H25, West Tower  
Alexandria, VA 22350-1500**

**DoD IG Subpoena Queue E-Mail Address: [subpoena@dodig.mil](mailto:subpoena@dodig.mil)**



### **CUSTODIAN LETTER**

The Custodian Letter is prepared by the DoD IG Subpoena Program Office and is addressed to the subpoena recipient. It explains the subpoena requirements and provides instructions for the subpoena recipient on return of service. The Custodian Letter contains contact information for the requestor and the signature block reflects the information identified for the reviewing supervisor unless otherwise noted by the requestor during the request process.

#### **(Agency Letterhead)**

##### **Custodian of Records**

**ACME Manufacturing Company  
ATTN: Legal/Subpoena Processing  
5000 West Washington Street  
Indianapolis, IN 46231**

**Dear Sir or Madam:**

**Pursuant to Title 5, United States Code, Section 406(a)(4), the enclosed subpoena duces tecum has been issued. The materials identified must be produced by the date and time indicated on the subpoena at the following address:**

**Office of Special Investigations  
OSI Detachment XXX  
ATTN: Special Agent John Public  
12345 Main Avenue  
XXXXXXX AFB, XX 12345**

**Should you elect to personally deliver the subpoenaed records, you will be required to attest to the completeness, accuracy, and authenticity of the documents produced. Or, upon request, Special Agent John Public or any Special Agent of the Office of Special Investigations (OSI) will personally assume custody of the required materials at your office. However, by mutual agreement, the material may be sent by U.S. registered mail to OSI at the above address. If you elect to provide records via registered mail, you should include the enclosed personal affidavit/certificate of compliance as to the completeness, accuracy and authenticity of the documents mailed. Should the documents fail to arrive by the time and date set forth in the subpoena, this will be considered a failure on your part to comply with this subpoena.**



Original documents are required by this subpoena. However, for the purpose of this subpoena, certified true copies of the original documents called for by the subpoena will satisfy this provision. The personal affidavit/certificate of compliance must be made by the actual custodian of records who has the complete legal standing for the company/corporation and can testify to their authenticity, accuracy, and completeness of the documents produced. If certified true copies are produced, we reserve the right to review the original documents with advanced notice, during normal business hours. Otherwise, original documents must be submitted.

Materials required by the subpoena should be accompanied by an index identifying each document or other materials and the item or items of the subpoena to which it relates. If for any reason any of the required materials are not furnished, prepare an itemized list of the location of materials and the reason for nonproduction.

This investigation is private and we request such privacy be maintained. Enclosed is a notice pursuant to the Privacy Act of 1974.

You should bear in mind you have the right to consult with and have an attorney represent you in this matter. If you have any questions concerning the subpoena or the materials required to be produced, you may contact Special Agent John Public via phone at (000) XXX-XXXX or at email address: [john.public@us.af.mil](mailto:john.public@us.af.mil).

Sincerely,

(Name and title of Special Agent in Charge/Commander)

Enclosures:

Subpoena Duces Tecum  
Appendix A  
Privacy Act Notice  
Certificate of Compliance



### ***Subpoena Duces Tecum***

The subpoena *duces tecum* is a command to a person or organization to appear at a specified time and place and to bring certain designated documents, to produce the documents, and to testify as to their authenticity as well as any other matter concerning which proper inquiry is made.

The *duces tecum* must have the correct legal name of the business or person being subpoenaed. Rule 45 of the Federal Rules of Civil Procedure states: "Serving a subpoena requires delivering a copy to the named person..."

The address for either a person or business must be a physical address and not a Post Office (PO) Box. If the recipient provides no other address than a PO Box then the subpoena and associated documents should be served via certified mail with a return receipt by UPS, FedEx or the US Postal Service. For businesses, the subpoena should be addressed to the Custodian of Records.

The subpoena will have your physical address for return of service. This is filled in by the DoD IG Subpoena Program Office in cooperation with the case agent.

DoD nexus, such as the DoD contract number, DoD program affected, etc., is included in the Description of Items. The required records can be listed on the subpoena or can be listed in an Appendix. Even if an Appendix is used, the subpoena is completed as part of the process to obtain a DoD IG Subpoena.

The Subpoena *Duces Tecum* is prepared by the DoD IG Subpoena Program Office.



United States of America  
Department of Defense  
Office of the Inspector General

**SUBPOENA DUCES TECUM**

TO Custodian of Records, ABC Corporation, 123 West Elm Street, Suite 144, New York, New York 12345-6789

YOU ARE HEREBY COMMANDED TO APPEAR BEFORE Special Agent Sam Spade, or any Special Agent of the Department of the Army Criminal Investigation Division (CID) acting on behalf of the Inspector General, pursuant to the Inspector General Act of 1978 (5 U.S.C. § 406(a)(4)), at CID, Street Address, City or Post, State 00000-0000 no later than 10 o'clock a.m. on the 31<sup>st</sup> day after receipt of the subpoena by the above named recipient.

You are hereby required to bring with you and produce at said time and place the following information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence pertaining to language identifying the DoD nexus and overall factors such as contract number, time period, etc., as specified in Appendix A, which are necessary in the performance of the responsibility of the Inspector General under the Inspector General Act.

**IN TESTIMONY WHEREOF**, the signature of the duly authorized representative of the Inspector General of the Department of Defense is affixed at Alexandria, Virginia.

\_\_\_\_\_  
Harvey Specter  
Associate General Counsel, Office of General Counsel

UNIQUE IDENTIFICATION NUMBER: 2023XXXX-XXXXX



## APPENDIX A

See Appendix B of this guide for a detailed explanation regarding the Appendix A.

The following Appendix A's and Appendix B are provided as samples. Please remember, requestor is not required to submit an Appendix A except for major procurement fraud investigations wherein documents are being subpoenaed from a Contractor/Subcontractor.

Requestor may request a template in Microsoft Word® format by sending an email to the DoD IG Subpoena Team at [subpoena@dodig.mil](mailto:subpoena@dodig.mil).





## **SAMPLE APPENDIX A – ISP, TELECOM/CELLULAR CARRIERS, AND SOCIAL MEDIA PLATFORMS (BASIC SUBSCRIBER INFORMATION)**

### **A. INSTRUCTIONS**

This subpoena calls for the production of records setting forth the basic subscriber information identified below, authorized by the Stored Communications Act (18 U.S.C. § 2701, et seq.), pertaining to [*email address/Internet Protocol (IP) address/username*]: [*insert targeted account information*], believed to be utilized by and/or associated with a member of the United States Armed Forces, who is suspected of violating one or more criminal statutes and/or punitive Articles of the Uniform Code of Military Justice, for the period January XX, 2023 through the date of this subpoena.

### **B. REQUIRED RECORDS**

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records (to include telephone call detail and text message detail records) and/or records of session times and durations, including connection dates and times, disconnect dates and times, and methods of connection;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol (“IP”) addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.



## SAMPLE APPENDIX A – FINANCIAL RECORDS (ABBREVIATED VERSION)

### A. DEFINITIONS:

1. The terms “document” or “documents” mean any written, recorded, graphic material of any kind, including photostats, microfilms, microfiche, tape or disc recordings, computer printouts and other data electronically obtained or otherwise stored from which information can be obtained, either directly, indirectly or by translation, through devices or readers, whether prepared by your or any other person, that is in your possession, custody or control. Any such document is to be produced in a reasonable useable form.

2. The terms “document” and “documents” include the original document (or copy thereof if the original is not in your possession, custody or control) and all copies that differ in any respect from the original or that bear any notation, marking or information not on the original.

3. The term “account(s)” means bank accounts, whether open or closed, including but not limited to checking accounts, savings accounts, and credit card accounts.

### B. DOCUMENTS REQUIRED:

This subpoena calls for the production of documents pertaining to any and all (*Financial Institution Name*) account(s) held solely or jointly by (*name*), Social Security Number: XXX-XX-1234, a member of the United States Armed Forces, who is suspected of violating one or more criminal statutes and/or punitive Articles of the Uniformed Code of Military Justice, for the period December 1, 2022 through the date of this subpoena.

1. Documents pertaining to all accounts, including but not limited to:
  - a. Documents reflecting account ownership in effect during the identified period, including signature cards;
  - b. Monthly account statements;
  - c. Automatic Teller Machine (ATM) withdrawal and point of sale debits;
  - d. Deposit tickets;
  - e. Copies of checks written on the named account and/or deposited into the named account;
  - f. Wire transfer documents; and
  - g. Form 1099, 1089, or back-up withholding documents.



## SAMPLE APPENDIX A – FINANCIAL RECORDS (EXPANDED VERSION)

### A. DEFINITIONS:

1. The terms “document” or “documents” mean any written, recorded, graphic material of any kind, including photostats, microfilms, microfiche, tape or disc recordings, computer printouts and other data electronically obtained or otherwise stored from which information can be obtained, either directly, indirectly or by translation, through devices or readers, whether prepared by your or any other person, that is in your possession, custody or control. Any such document is to be produced in a reasonable useable form.

2. The terms “document” and “documents” include the original document (or copy thereof if the original is not in your possession, custody or control) and all copies that differ in any respect from the original or that bear any notation, marking or information not on the original.

3. The term “account(s)” means bank accounts, whether open or closed, including but not limited to checking accounts, savings accounts, and credit card accounts.

### B. DOCUMENTS REQUIRED:

This subpoena calls for the production of documents pertaining to any and all (*Financial Institution Name*) account(s) to include account number: **12345678910**, held solely or jointly by (*name*), Social Security Number: XXX-XX-1234, a member of the United States Armed Forces, who is suspected of violating one or more criminal statutes and/or punitive Articles of the Uniformed Code of Military Justice, for the period December 1, 2022 through the date of this subpoena.

1. Documents pertaining to all accounts, including but not limited to:
  - a. Documents reflecting account ownership in effect during the identified period, including signature cards;
  - b. Monthly account statements;
  - c. Automatic Teller Machine (ATM) withdrawal and point of sale debits;
  - d. Deposit tickets;
  - e. Copies of checks written on the named account and/or deposited into the named account;
  - f. Wire transfer documents; and
  - g. Form 1099, 1089, or back-up withholding documents.



2. Documents pertaining to all cashier's, manager's, or bank checks, traveler's checks, and money orders purchased or negotiated by any of the named parties or entities, including but not limited to:

- a. Documents (checks, debit memos, cash in tickets, wires in, etc.) reflecting the means by which the checks or money orders were purchased;
- b. Documents, including bank checks, credit memos, cash out tickets, wires out, etc., reflecting disbursements of the proceeds of any negotiated checks or money orders;
- c. Applications for purchase of checks or money orders; and
- d. Copies of negotiated checks or money orders.

3. Documents pertaining to wire transfers sent or received by any of the names parties or entities, including but not limited to:

- a. Fed Wire, CHIPS, SWIFT, or other money transfer of message documents;
- b. Documents, including checks, debit memos, cash in tickets, wires in, etc., reflecting the source of the funds wired out;
- c. Documents, including bank checks, credit memos, cash out tickets, wires out, etc., reflecting the ultimate disposition within the bank of the funds wired in; and
- d. Notes, memoranda, or other writings pertaining to the sending or receipt of wire transfers.

4. Documents pertaining to electronic device and account access, including but not limited to:

- a. Source IP address with date/time stamp of online-based banking account creation and/or activation;
- b. Source device information for account access from mobile banking applications, including mobile device type/model used, telephone number, and International Mobile Equipment Identity Number (IMEI), with associated date/time stamps of ALL activity;
- c. Source device information for account access from a personal computer, including PC type/model/operating system used and Media Access Control (MAC) address, with associated date/time stamps of ALL activity; and
- d. Source IP address and date/time of web-based activity for ALL online banking activity with date/time stamp.



## **SAMPLE APPENDIX A – MAJOR PROCUREMENT FRAUD INVESTIGATIONS**

### **APPENDIX A (Insert Company's Name)**

#### **I. DEFINITIONS**

1. "Document(s)" means, without limitation, any written, printed, typed, photographed, recorded, or otherwise reproduced or stored communication or representation, whether comprised of letters, words, numbers, pictures, sounds or symbols, or any combination thereof. This definition includes copies or duplicates of documents contemporaneously or subsequently created which have any non-conforming notes or other markings and the backsides of any communication or representation which all contain any of the above. "Document(s)" includes, but is not limited to: Correspondence; memoranda; notes; drafts; records; letters; envelopes; telegrams; messages; electronic mail; analyses; agreements; accounts; working papers; reports and summaries of investigations; trade letters; press releases; comparisons; books; notices; drawings; diagrams; instructions; manuals; calendars; diaries; articles; magazines; newspapers; brochures; guidelines; notes or minutes of meetings or of other communications of any type, including inter- and intra-office or company communications; questionnaires; surveys; charts; graphs; photographs; films or videos; tapes; discs; data cells; bulletins; printouts of information stored or maintained by electronic data processing or word processing equipment; electronic claims filing, invoices, all other data compilations from which information can be obtained including electromagnetically sensitive stored media such as floppy discs, hard discs, hard drives and magnetic tapes; and any preliminary versions, drafts or revisions of any of the foregoing.

2. The term "document(s)" also means any container, file folder, or other enclosure bearing any marking or identification in which other "documents" are kept, but does not include file cabinets. In all cases where any original or non-identical copy of any original is not in the possession, custody, or control of the company, the term "document(s)" shall include any copy of the original and any non-identical copy thereof.

3. "DoD" refers to the United States Department of Defense, including any and all departments, agencies, and subordinate organizations thereof.



4. “USMC” refers to the United States Marine Corps, including any and all departments, agencies, and subordinate organizations thereof.

5. “DCIS” means the Defense Criminal Investigative Service.

6. “Company Name” means (Company’s Full Name) Incorporated and any subsidiaries, affiliates, d/b/a, predecessor-in-interest, any wholly or partially owned subsidiary, or other affiliated companies or businesses, segments, divisions, or other units, whatsoever titled, both presently existing and those which previously existed, and any present or former officers, directors, employees, consultants, contractors, agents, or members of the board of directors and any other persons working for or on behalf of the foregoing at any time during the period covered by this subpoena.

7. “Secondary Company Name” means (Company’s Full Name) and any subsidiaries, affiliates, d/b/a, predecessor-in-interest, any wholly or partially owned subsidiary, or other affiliated companies or businesses, segments, divisions, or other units, whatsoever titled, both presently existing and those which previously existed, and any present or former officers, directors, employees, consultants, contractors, agents, or members of the board of directors and any other persons working for or on behalf of the foregoing at any time during the period covered by this subpoena.

8. “You” or “your” means the person or entity listed as the recipient of this subpoena. If an entity, “you” or “your” includes any parents, subsidiaries, affiliates, segments, divisions, both presently existing and those which previously existed, of such entity, and any present or former officers, directors, employees, consultants, contractors, attorneys, agents, and members of the board of directors of any of the foregoing entities. If a person, “you” or “your” includes your attorneys, representatives, agents, and all persons or entities acting or purporting to act on your behalf.

9. The term “Contract(s)” or “Contract(s) at Issue” means contract number(s) M00123-08-D-001 between (Company Name) and the USMC, and all modifications and/or extensions to the Contracts at Issue.

10. The term “Subcontract(s)” or “Subcontract(s) at Issue” means contract(s) between (Company Name) and any subcontractor in support of the Contracts at Issue, and all modifications and/or extensions to the Subcontract at Issue.



11. The terms “with regard to,” “regarding,” “relates,” “relating to,” “referencing,” and “concerning” means relating to, regarding, constituting, referring to, reflecting, describing, embodying, showing, discussing, evidencing, or in any way pertaining to.

12. The words “and” and “or” in this subpoena shall be read in both the conjunctive and the disjunctive (i.e., “and/or”), so as to give the document request the broadest meaning.

13. The term “any and all” means all documents and records that respond in whole or in part to any part or clause of any paragraph of this subpoena, and shall be produced in their entirety, including all attachments and enclosures. The term “any” shall be construed to include the word “all” and the term “all” shall be construed to include the word “any.”

14. The terms “technical publication” and “technical publications” mean any and all technical orders, time compliance technical orders, country standards, military specifications (MILSPEC), Federal specifications (FEDSPEC) and any other technical manual, book, or publication which (Company Name) used and/or relied upon when performing work under the contract.

15. “Concerning” means referring to, describing, evidencing, or constituting.

16. “Communication” means the transmittal of information (in the form of facts, ideas, inquiries, or otherwise).

17. The term “correspondence” means any recorded material from one individual or entity to another, to include, but not limited to, electronic mails, notes, letters, telephone logs, facsimile, facsimile logs, voice recordings or other form of communication.

## II. INSTRUCTIONS

1. The recipient of this subpoena shall identify a qualified custodian of records who may be required to appear and testify at a date to be determined in the future concerning the production and authentication of documents and records required to be produced by this subpoena.

2. If a claim of privilege is asserted in response to any document requested by this subpoena, and such document, or any part thereof, is not produced on the basis of such claim, for each such document or part thereof that is not produced, you are directed to provide a





privilege log. In the log, you should identify the type of document being withheld (for example, letter, memorandum, handwritten notes, marginalia, etc.), all actual and intended recipients of the document, its date, and the specific privilege being asserted, all with sufficient particularity so as to comply with Federal Rule of Civil Procedures 26(b)(5). In addition, where a document is pulled for privilege, please insert a colored piece of paper containing the same bates-number as the document pulled so that it is clear from whose files the privileged documents were pulled.

3. Scope of Search Required: This subpoena calls for all documents in your possession, custody, or control, including, but not limited to, documents in the possession of your officers, directors, employees, agents, and consultants. You are required to search all files, including electronic sources, reasonably likely to contain responsive documents, including files left behind by former officers, directors, agents, and employees or those that are otherwise in the possession, custody, or control of (Company Name).

4. Electronic Records: Unless kept in electronic format in the ordinary course of business, all documents provided in response to this subpoena must be the original paper documents, to include all copies that differ in any respect (such as marginalia and/or notations), and all markings and post-it notes and other similar documents attached thereto, as well as all attachments referred to or incorporated by the documents. To the extent that the Department of Defense Inspector General agrees to accept duplicates of any original paper document, such copies must be exact duplicates of the original in format and substance, to include all staples, paper clips, files, labels, marginalia, and condition as single or double-sided documents. To the extent records are kept electronically in the normal course of business, they are required to be produced in that format, with sufficient identification of software and provision of any proprietary software as required to access and manipulate the documents to the same extent accessed and manipulated by (Company Name). Questions concerning the compatibility of the software should be addressed with Special Agent \_\_\_\_\_ at phone number: \_\_\_\_\_ or via email address: \_\_\_\_\_. For more detailed information regarding productions of electronic documents, see **Appendix B**.

5. Manner of Production: All documents produced in response to this subpoena shall comply with the following instructions:

- a. You shall conduct a search for responsive documents in a manner sufficient to identify the source and location where each responsive document is found.
- b. All documents produced in response to this subpoena shall be segregated and labeled to show the document request to which the documents are responsive and the source and location where the document was found.





c. To the extent that documents are found in file folders, computer disks, hard drives and/or other storage media which have labels or other identifying information, the documents shall be produced with such file folder and label information intact.

6. To the extent that documents are found attached to other documents, by means of paper clips, staples, or other means of attachment, such documents shall be produced together in their condition when found.

7. All records responsive to this subpoena are required, regardless of media involved (e.g., paper, electronic, magnetic, photo-optical, or other). Electronic records must be provided in a useable storage device such as a compact disk. Identify the computer software used to create, manipulate, and/or operate all electronic data.

8. The singular form of a word shall be construed to include within its meaning the plural form of the word, and vice versa, and the use of any tense of any verb shall be considered to also include all other tenses.

9. Notwithstanding the language of numbered paragraph II. 4. above, copies may be provided in response to this subpoena. If copies are provided, the originals must be maintained and safeguarded and made available to us on request.

10. In the event there are no documents responsive to a particular subpoena request, please specify that you have no responsive documents.

11. If you know of documents you once possessed or controlled, but no longer possess or control, which would have been responsive to this subpoena, state what disposition was made of such documents, including identification of the persons who are or are believed to be in possession or control of such documents currently.

12. To facilitate the handling and return of the submitted documents, please mark each page with an identifying logo or the first three letters of your company's name and number each page sequentially beginning with "00001." The marks should be placed in the lower right hand corner of each page but should not obscure any information on the document. All documents should be produced in enclosures bearing your name, the date of the subpoena, and the paragraph(s) of the subpoena to which the documents respond.

13. To the extent that (Company Name) claims that documents produced fall within the scope of the Trade Secrets Act (18 U.S.C. § 1905), the Freedom of Information Act (5 U.S.C. §



552), or other statutory or common law provision that purports to regulate the ability of the United States to handle and make use of the document, you must mark each passage(s) or page(s) with a legend that clearly identifies the basis of your claim; e.g., “TSA – Trade Process Information,” “TSA – Income Information,” “FOIA Exemption 4.”

14. Production shall be made in such a manner as to ensure that Special Agents of the XXXX (Your DCIO abbreviation) may readily determine the source and location of each document.

15. Upon completion of the production of documents and records pursuant to this subpoena, the recipient (if the recipient is an individual, then that individual; if the recipient is a corporation, then a corporate officer; if the recipient is a partnership, then a partner; if the recipient is a sole proprietorship, then the owner) shall complete and execute the Certificate of Compliance accompanying this subpoena and deliver same to the individual at location identified on the face of the subpoena. Failure to complete and execute the Certificate of Compliance shall be deemed willful non-compliance with the subpoena.

### **III. TIME PERIOD**

Unless otherwise indicated, the relevant time period for each document request in this subpoena shall be from (inclusive dates), and shall include all documents created, prepared, dated, sent, received, altered, in effect, or which came into existence during this period, or which refer or relate to that period, regardless of when the documents were created or prepared.

### **IV. DOCUMENTS REQUIRED**

This subpoena requires the production of documents or categories of documents associated with the Contracts/Subcontracts at Issue, identified below:

1. Any and all general ledgers with general journal entries, including adjusting and reversing entries; payable journals, including invoices and corresponding documentation; purchase journals, including purchase orders, purchasing files, receiving reports, and vendor quotes; and receivable journals and sales journals, including corresponding documentation as it pertains to the Contracts/Subcontracts at Issue.



2. Any and all supporting documentation for interest expenses, travel and entertainment expenses, officers' life insurance, and commission expenses.

3. Any and all labor records, including, but not limited to, the labor hour monthly accumulation and distribution books, job distribution reports, time cards, certified payroll registers, canceled payroll checks and bank statements, automated data processing summaries, and all corresponding source documents.

4. Any and all direct and indirect labor rates and hours, with corresponding support documents.

5. Any and all canceled checks and bank statements for accounts of (Company Name).

6. Any and all inventory files and analyses.

7. Any and all manufacturing, engineering and labor overhead, and cost of money rate submissions, with listings of all items, costs, and expenses used to calculate those rates.

8. Any and all internal monthly, quarterly and/or annual financial reports, audited financial statements, with all footnotes, and auditing working papers and files.

9. Any and all personnel records for officers and employees. In lieu of producing all responsive documents, a list that includes the following data will be accepted: Full name, current or last known address, home telephone numbers, date of birth, Social Security number, employment and education history, position, position description to include type of employment (for example, full-time/part-time/freelancer/etc.), and job titles.

10. Any and all contract/subcontract files pertaining to the DoD contract including, but not limited to, quotes, bid proposals, contracts, progress payments, DD Forms 250, and correspondence.

11. Any and all documentation pertaining to inspections of work performed by (Company Name) for Contracts/Subcontracts at Issue.

12. Any and all (Company Name) policies and procedures manuals.

13. Any and all corporate internal audit reports, with working papers and management responses.



14. Any and all documents pertaining to negotiations between (Company Name) and the DoD and/or prime contractors.

15. Weekly time reports prepared by all employees. Any and all time reports generated by the weekly time report that is prepared by each employee, to include how employees log/submit their hours and the review/approval of employee hours.

16. Company benefits paid on behalf of each employee during the period requested.

17. All public vouchers (SF 1034), with applicable delivery orders, related project numbers, and voucher support for each contract.

18. All subcontract agreements with applicable support relevant to the Contracts/Subcontracts at Issue.

19. Information sufficient to identify any and all customers, both commercial and Government, with whom (Company Name) worked with in support of the Contracts/Subcontracts at issue.

20. Information sufficient to identify all (Company Name) employees who have worked on DoD contracts from December 1, 2007, to the date of this subpoena.



## **SAMPLE APPENDIX B – DIGITAL MEDIA SPECIFICATIONS MAJOR PROCUREMENT FRAUD INVESTIGATIONS**

### **APPENDIX B**

#### **Specifications for Production of ESI and Digitized (“Scanned”) Images (“Production Specifications”)**

##### **Collection of Electronically Stored Information (ESI)**

Careful consideration should be given to the methodology, implementation and documentation of ESI collection to ensure that all responsive data and metadata are preserved in the collection process. Consideration should also be given as to whether production media should be encrypted when producing to the government when required by law (i.e. Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), etc. *See* Section 20 below.

#### **1. Specification Modifications**

Any modifications or deviations from the Production Specifications may be done only with the express permission of the government and these modifications or deviations should be communicated to the government and approved by the government in written form. Any responsive data or documents that exist in locations or native forms not discussed in these Production Specifications remain responsive and, therefore, arrangements should be made with the government to facilitate their production.

#### **2. Production Format of ESI and Imaged Hard Copy Documents**

Responsive ESI and imaged hard copy shall be produced in the format outlined below. All ESI, except as outlined below in sections 5 – 16, shall be rendered to TIFF image format, and accompanied by an Opticon/Concordance® Image Cross Reference file. All applicable metadata/database (see section 3 below) shall be extracted and provided in Concordance® load file format.

- a. Image File Format:** All documents shall be produced in black and white TIFF format unless the image requires color. An image requires color when color in the document adds emphasis to information in the document or is itself information that would not be readily apparent on the face of a black and white image.
- b.** When producing black and white paper documents scanned to images, or rendered ESI, they shall be produced as 300 dpi, 1 bit, single-page TIFF files, CCITT Group IV (2D Compression). When producing in *color*, paper documents scanned to images, or rendered



ESI, they shall be produced as 300 dpi single-page JPG. Images should be uniquely and sequentially Bates numbered and unless otherwise specified, Bates numbers should be an endorsement on each image.

- i. All TIFF file names shall include the unique Bates number burned into the image. (See Section 1, below, regarding Bates number instructions.)
  - ii. All TIFF image files shall be stored with the “.tif” extension.
  - iii. Images shall be OCR’d using standard COTS products.
    1. An exception report shall be provided when limitations of paper digitization software/hardware or attribute conversion do not allow for OCR text conversion of certain images. The report shall include the DOCID or Bates number(s) corresponding to each such image.
  - iv. All pages of a document or all pages of a collection of documents that comprise a folder or other logical grouping, including a box, shall be delivered on a single piece of media.
  - v. No image folder shall contain more than 2,000 images.
- c. **Opticon/Concordance® Image Cross Reference file:** Images should be accompanied by an Opticon load file that associates each Bates number with its corresponding single-page TIFF image file. The Cross Reference file should also contain the relative image file path for each Bates numbered page. The Opticon/Concordance® Image Cross Reference file is a page level load file, with each line representing one image.

Below is a sample:

```
REL000000001,,.\IMAGES\001\REL000000001.TIF,Y,,,
REL000000002,,.\IMAGES\001\REL000000002.TIF,,,
REL000000003,,.\IMAGES\001\REL000000003.TIF,,,
REL000000004,,.\IMAGES\001\REL000000004.TIF,Y,,,
REL000000005,,.\IMAGES\001\REL000000005.TIF,,,
```

The fields are, from left to right:

- Field One – (REL000000001) – the Bates Number. This value must be unique for each row in the OPT file. The first page of each document must match the DOCID or BEGDOC# value of the respective document.
- Field Two – (blank) – the volume identifier. This field is not required.
- Field Three – (.\\IMAGES\\001\\REL000000001.TIF) – The relative file path to the image to be loaded.
- Field Four – (Y) – the document marker. A “Y” indicates the start of a unique document.
- Field Five – (blank) – The folder indicator. This field is not required, and typically is not used.



- Field Six – (blank) – The box indicator. This field is not required, and typically is not used.
- Field Seven – (blank) – The page count. This field is not required.

**d. Concordance® Load File:** Images should also be accompanied by a flat, document-level load file to provide the metadata and native files containing delimited text that will populate fields in a searchable, flat database environment. The file encoding must be one of four types: Western European (Windows), Unicode (UTF16), Big-Endian Unicode, or UTF8. The file should contain the required fields listed below in Section 3.

1. Text delimited load files are defined using the standard Concordance delimiters. For example:

|                        |                      |
|------------------------|----------------------|
| <i>Field Separator</i> | <i>¶ or Code 020</i> |
| <i>Text Qualifier</i>  | <i>þ or Code 254</i> |
| <i>Newline</i>         | <i>® or Code 174</i> |
| <i>Multi-value</i>     | <i>° or Code 167</i> |
| <i>Nested values</i>   | <i>\ or Code 092</i> |

2. This load file should contain the relative file path to the individual multi-page, document level text files.
3. This load file should also contain the relative file path to all provided native files, such as Microsoft Excel or PowerPoint files.
4. There should be one line for every record in a collection.
5. The load file must contain a header listing the metadata/database fields contained within. For example, if the data file consists of a First Page of a Record (BegDoc#), Last Page of a Record (ending Bates / ENDDOC#), DOCID, DOCDate, File Name, and a Title, then the structure may appear as follows:

`þBEGDOCþ¶þENDDOCþ¶þDOCIDþ¶þDOCDATEþ¶þFILENAMEþ¶þTITLEþ`

- e. The extracted/OCR text** should be provided for each document as a separate single text file. The file name should match the BEGDOC# or DOCID for that specific record and be accompanied by the .txt extension.
- f. Directory and folder structure:** The directory structure for productions should be:

`\CaseName\LoadFiles`

`\CaseName\Images` < For supporting images (can include subfolders as needed, should not include more than 2,000 files per folder)

`\CaseName\Natives` <Native Files location (can include subfolders as needed, should not include more than 2,000 files per folder)



\CaseName\Text <Extracted Text files location (can include subfolders as needed, should not include more than 2,000 files per folder)

\CaseName\Translated Images < For supporting images of translated documents (as needed for rendered translated documents; can include subfolders as needed, should not include more than 2,000 files per folder)

\CaseName\Translated Text <Translated Text files location (as needed for translated text; can include subfolders as needed, should not include more than 2,000 files per folder).

### 3. Required Metadata/Database Fields

A “√” denotes that the indicated field should be present in the load file produced. “Other ESI” includes data discussed in Sections 5 – 16 below, but does not include e-mail, e-mail repositories (Section 11), “stand alone” items (Section 12), and imaged hard copy material (Section 9). E-mail, e-mail repositories, and “stand alone” materials (Section 12) should comply with “E-mail” column below. Imaged hard copy materials should comply with the “Hard Copy” column. The parties will meet and confer about any field which cannot be populated automatically (i.e. would require manual population of information).

| Field name              | Field Description  | Field Type | Field Value | Hard Copy | E-Mail | Other ESI |
|-------------------------|--|------------|-------------|-----------|--------|-----------|
| COLLECTION SOURCE       | Name of the Company/Organization data was collected from   | Text       | 160         | √         | √      | √         |
| SOURCE ID (BOX #)       | Submission/volume/box number   | Text       | 10          | √         | √      | √         |
| CUSTODIAN               | Custodian/Source - format: Last, First or ABC Dept.  | Text       | 160         | √         | √      | √         |
| DUPECUSTODIAN           | Custodian/Source – all custodians who had the document before de-duplication; format: Last, First or ABC Dept. | Text       | Unlimited   |           | √      | √         |
| DUPECUSTODIAN FILE PATH | Listing of all the file locations of the document before de-duplication  | Text       | Unlimited   |           | √      | √         |
| AUTHOR                  | Creator of the document  | Text       | 500         |           |        | √         |
| BEGDOC#                 | Start Bates (including prefix) - No spaces   | Text       | 60          | √         | √      | √         |
| ENDDOC#                 | End Bates (including prefix) - No spaces   | Text       | 60          | √         | √      | √         |





| Field name  | Field Description   | Field Type                 | Field Value | Hard Copy | E-Mail | Other ESI |
|-------------|---|----------------------------|-------------|-----------|--------|-----------|
| DOCID       | Unique document Bates # or populate with the same value as Start Bates (DOCID = BEGDOC#)  | Text                       | 60          | ✓         | ✓      | ✓         |
| PGCOUNT     | Page Count  | Number                     | 10          | ✓         | ✓      | ✓         |
| GROUPID     | Contains the Group Identifier for the family, in order to group files with their attachments  | Text                       | 60          |           | ✓      | ✓         |
| PARENTID    | Contains the Document Identifier of an attachment's parent  | Text                       | 60          |           | ✓      | ✓         |
| ATTACHIDS   | Child document list; Child DOCID or Child Start Bates   | Text – semicolon delimited | Unlimited   | ✓         | ✓      | ✓         |
| ATTACHLIST  | List of Attachment filenames  | Text – semicolon delimited | Unlimited   |           | ✓      | ✓         |
| BEGATTACH   | Start Bates number of parent  | Text                       | 60          | ✓         | ✓      | ✓         |
| ENDATTACH   | End Bates number of last attachment   | Text                       | 60          | ✓         | ✓      | ✓         |
| PROPERTIES  | Privilege notations, Redacted, Document Withheld Based On Privilege   | Text – semicolon delimited | Unlimited   | ✓         | ✓      | ✓         |
| RECORD TYPE | Use the following choices: Image, Loose E-Mail, E-Mail, E-Doc, Attachment, Hard Copy or Other. If using Other, please specify what type after Other | Text                       | 60          | ✓         | ✓      | ✓         |
| FROM        | Sender (i.e.: E-Mail address, Last name, First name)  | Text                       | 160         |           | ✓      | ✓         |
| TO          | Recipient (i.e.: E-Mail address, Last name, First name)   | Text – semicolon delimited | Unlimited   |           | ✓      | ✓         |



| Field name     | Field Description   | Field Type                 | Field Value            | Hard Copy | E-Mail | Other ESI |
|----------------|---|----------------------------|------------------------|-----------|--------|-----------|
| CC             | Carbon Copy Recipients (i.e.: E-Mail address, Last name, First name)  | Text – semicolon delimited | Unlimited              |           | ✓      | ✓         |
| BCC            | Blind Carbon Copy Recipients (i.e.: E-Mail address, Last name, First name)  | Text – semicolon delimited | Unlimited              |           | ✓      | ✓         |
| SUBJECT        | Subject line of E-Mail  | Text                       | Unlimited              |           | ✓      |           |
| TITLE          | Document title  | Text                       | Unlimited              |           |        | ✓         |
| CONVINDE       | E-mail system ID used to track replies, forwards, etc.  | Text                       | Unlimited              |           | ✓      |           |
| DOCDATE        | Last Modified Date for files and Sent date for e-mail, this field inherits the date for attachments from their parent. Do not provide 00/00/0000.   | Date                       | MM/DD/YYYY             |           | ✓      | ✓         |
| TEXT FILEPATH  | Relative file path of the text file associated with either the extracted text or the OCR  | Text                       | Unlimited              | ✓         | ✓      | ✓         |
| DATE TIME SENT | Date and time Sent (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000. | Date and Time              | MM/DD/YYYY<br>HH:MM:SS |           | ✓      |           |
| DATE TIME CRTD | Date Created (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000.       | Date and Time              | MM/DD/YYYY<br>HH:MM:SS |           | ✓      | ✓         |



| Field name       | Field Description   | Field Type    | Field Value            | Hard Copy | E-Mail | Other ESI |
|------------------|---|---------------|------------------------|-----------|--------|-----------|
| DATE TIME SVD    | Date Saved (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000.                       | Date and Time | MM/DD/YYYY<br>HH:MM:SS |           | ✓      | ✓         |
| DATE TIME MOD    | Date Last Modified (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000.               | Date and Time | MM/DD/YYYY<br>HH:MM:SS |           | ✓      | ✓         |
| DATE TIME RCVD   | Date Received (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000.                    | Date and Time | MM/DD/YYYY<br>HH:MM:SS |           | ✓      |           |
| DATE TIME ACCD   | Date Accessed (USE TIME ZONE OF COLLECTION LOCALITY)<br>Numbers must be populated. If date is unknown, leave blank. Do not provide 00/00/0000.                    | Date and Time | MM/DD/YYYY<br>HH:MM:SS |           | ✓      | ✓         |
| TIME ZONE OFFSET | Time zone of collection locality, relative to Coordinated Universal Time (UTC). E.g., for US Central Standard Time (CST), the value for this field should be -6.0 | Decimal       | 10                     |           | ✓      |           |
| FILE SIZE        | Native File Size in KBs   | Decimal       | 10                     |           |        | ✓         |



| Field name     | Field Description   | Field Type | Field Value | Hard Copy | E-Mail | Other ESI |
|----------------|---|------------|-------------|-----------|--------|-----------|
| FILE NAME      | File name - name of file as it appeared in its original location  | Text       | Unlimited   |           |        | ✓         |
| APPLICATION    | Application used to create native file (e.g., Excel, Outlook, Word)   | Text       | 160         |           | ✓      | ✓         |
| FILE EXTENSION | Extension for the file (e.g., .doc, .pdf, .wpd)   | Text       | 10          |           | ✓      | ✓         |
| FILEPATH       | Data's original source full folder path   | Text       | Unlimited   |           | ✓      | ✓         |
| NATIVE LINK    | Relative file path location to the native file  | Text       | Unlimited   |           | ✓      | ✓         |
| FOLDER ID      | Complete E-Mail folder path (e.g., Inbox\Active) or Hard Copy container information (e.g., folder or binder name)   | Text       | Unlimited   | ✓         | ✓      |           |
| HASH VALUE     | Identifying value of an electronic record that is used for deduplication during processing. MD5 or SHA1 hash algorithms may be used, but must be kept consistent throughout all productions and communicated to government. | Text       | Unlimited   |           | ✓      | ✓         |
| MESSAGEHEADER  | E-mail header. Can contain IP address   | Text       | Unlimited   |           | ✓      |           |
| ATTACHMCOUNT   | Number of attachments (any level child document) associated with a ParentID   | Text       | 10          |           | ✓      |           |



| Field name          | Field Description  | Field Type | Field Value | Hard Copy | E-Mail | Other ESI |
|---------------------|--|------------|-------------|-----------|--------|-----------|
| FILE TYPE           | Description that represents the file type to the Windows Operating System. E.g., Adobe Portable Document Format, Microsoft Word 97 – 2003, or Microsoft Office Word Open XML Format. | Text       | 160         |           | ✓      | ✓         |
| HAS HIDDEN CONTENT  | Identifies whether the document has comments, track changes or other hidden content associated with it.  | Text       | Yes/No      |           | ✓      | ✓         |
| MESSAGE TYPE        | Exchange Message class or equivalent   | Text       | 60          |           | ✓      |           |
| EXTENDED PROPERTIES | For PDFs Only  | Text       | Unlimited   |           | ✓      | ✓         |
| HAS REDACTIONS      | Identifies whether a record has been produced with redactions; should be populated with Y for records with redactions and N for records without redactions.                          | Text       | Yes/No      | ✓         | ✓      | ✓         |

#### 4. Search, De-Duplication, Near-Duplicate Identification, Technology Assisted Review, E-mail Conversation Threading, and Other Culling Procedures

- a. De-duplication of exact hash copies shall be performed globally – across all custodians. The custodian of each record shall be populated in the DupeCustodian field.
- b. All files found on the National Institute of Standards and Technology (NIST) list, commonly referred to as deNISTing, should be excluded from delivery to the government. All available metadata from files withheld from delivery due to the deNISTing process will be available upon request.
- c. All files should be globally de-duplicated with the following conditions:
  - i. The “DupeCustodian” metadata field (listing of all custodians who had the document before de-duplication) must be provided with the document production.



- ii. The “DupeCustodian File Path” metadata field (listing all the file locations of the document before de-duplication) must be provided with the document production.
  - iii. All files and metadata for the duplicate documents removed during de-duplication must be preserved and available for production upon request.
  - iv. No customization of hashing may occur without prior express approval by the government.
  - v. De-duplication must be done by document family, not by individual document.
  - vi. A detailed description of the steps taken to de-duplicate (including the process of obtaining hash values) must be provided to the government. For every production after the first, a separate Unified Custodian overlay shall be provided. If no overlay is necessary due to the fact that no documents de-duped out in connection with previously produced documents, this shall be expressly stated in the cover letter accompanying the subsequent production(s).
- d. The recipient shall not use any other procedure to cull, filter, group, separate or de-duplicate, or near-deduplicate, etc. (i.e., reduce the volume of) responsive material before discussing with and obtaining the written approval of the government. All objective coding (e.g., near-duplicate ID or e-mail thread ID) shall be discussed and produced to the government as additional metadata fields. The recipient will not employ analytic software or technology to search, identify, or review potentially responsive material, including but not limited to, technology assisted review or predictive coding, without first discussing with the government.

## **5. Hidden Text**

All hidden text (e.g. track changes, hidden columns, mark-ups, notes) shall be expanded and rendered in the image file. Except for Adobe PDF files, for any files that cannot be expanded, the native files shall be produced with the image file. If an Adobe PDF’s hidden text cannot be expanded and rendered in an image file, it need only be produced in native form if individually requested by a specific document identifier or bates number.

## **6. Embedded Files**

All non-graphic embedded objects (Word documents, Excel spreadsheets, .wav files, etc.) that are found within a file shall be extracted and produced. For purposes of production, the embedded files shall be treated as attachments to the original file, with the parent/child relationship preserved.

The parties shall meet and confer regarding how to treat file links, including links within e-mails to centralized document repositories (e.g. MS OneDrive and Google Drive).

## **7. Image-Only Files**

All image-only files (non-searchable .pdfs, multi-page TIFFs, Snipping Tool and other screenshots, etc., as well as all other images that contain text) shall be produced with OCR text and metadata/database fields identified in section 3 for “Other ESI.”



## **8. Encrypted Files**

Any data (whether individual files or digital containers) that is protected by a password, encryption key, digital rights management, or other encryption scheme, shall be decrypted prior to processing for production.

- a. The unencrypted text shall be extracted and provided per Section 2.d. The unencrypted files shall be used to render images and provided per Sections 2.a and 2.b. The unencrypted native file shall be produced pursuant to Sections 10 – 16.
- b. If such protected data is encountered but unable to be processed, each file or container shall be reported as an exception in the accompanying Exception Report (pursuant to Section 23) and shall include all available metadata associated with the data, including custodian information.

## **9. Production of Imaged Hard Copy Records**

All imaged hard copy material shall reflect accurate document unitization including all attachments and container information (to be reflected in the PARENTID, ATTACHID, BEGATTACH, ENDATTACH and FOLDERID).

- a. Unitization in this context refers to identifying and marking the boundaries of documents within the collection, where a document is defined as the smallest physical fastened unit within a bundle. (e.g., staples, paperclips, rubber bands, folders, or tabs in a binder).
- b. The first document in the collection represents the parent document and all other documents will represent the children.
- c. All imaged hard copy documents shall be produced as 300 dpi single-page TIFF files, CCITT Group IV (2D Compression). All documents shall be produced in black and white TIFF format unless the image requires color. An image requires color when color in the document adds emphasis to information in the document or is itself information that would not be readily apparent on the face of a black and white image. Images identified as requiring color shall be produced as color 300 dpi single-page JPEG files.
- d. All objective coding (e.g., document date or document author) should be discussed and could be produced to the government as additional metadata/database fields should they be deemed as necessary.

## **10. Production of Spreadsheets and Presentation Files**

All spreadsheet and presentation files (e.g., Excel, PowerPoint) shall be produced in the unprocessed “as kept in the ordinary course of business” state (i.e., in native format), with an associated placeholder image and endorsed with a unique Bates number. *See* Section 17 below. The file produced should maintain the integrity of all source, custodian, application, embedded, and related file system metadata.



### **11. Production of E-mail Repositories**

E-mail repositories, also known as e-mail databases (e.g., Outlook PST, Lotus NSF), can contain a variety of items, including messages, calendars, contacts, tasks, etc. E-mail database systems should not be produced without consultation with and written consent of the government about the format for the production of such databases.

### **12. Production of Items Originally Generated in E-mail Repositories but Found and Collected Outside of E-mail Repositories, i.e., “Stand-alone” Items**

Any parent e-mail or other parent items (e.g., calendar, contacts, tasks, notes, etc.) found and collected outside of e-mail repositories (e.g., items having extensions .msg, .htm, .mht, etc.), shall be produced with the “Loose E-mail” metadata fields outlined in Section 3, including but not limited to any attachments, maintaining the family (parent/child) relationship.

### **13. Production of Structured Data**

Prior to any production of responsive data from a structured database (e.g., Oracle, SAP, SQL, MySQL, QuickBooks, proprietary timekeeping, accounting, sales rep call notes, CRMs, SharePoint, etc.), the producing party shall first identify the database type and version number, discuss providing the database dictionary (in whole or part) and any user manuals, or any other documentation describing the structure and/or content of the database and a list of all reports that can be generated from the database. Upon consultation with and written consent of the government, the standard format of all reports provided should be in comma separated values (.csv) format. The information that will be contained in the reports must be thoroughly explained to the government before production.

### **14. Production of Photographs with Native File or Digitized ESI**

Photographs shall be produced as single-page JPEG files with a resolution equivalent to the original image as they were captured/created. All JPEG files shall have extracted metadata/database fields provided in a Concordance® load file format as outlined in Section 3 for “Other ESI.”

### **15. Production of Images from which Text Cannot be OCR Converted**

An exception report shall be provided when limitations of paper digitization software/hardware or attribute conversion do not allow for OCR text conversion of certain images. The report shall include the DOCID or Bates number(s) corresponding to each such image.

### **16. Production of Native Files (When Applicable Pursuant to These Specifications)**

Production of native files, as called for in these specifications, shall have extracted metadata/database fields provided in a Concordance® load file format as defined in the field specifications for “Other ESI” as outlined in Section 3 as well as a placeholder image which indicates a native file is being produced.

ESI shall be produced in a manner which is functionally usable by the government. The following are examples:





- a. AutoCAD data, e.g., DWG and DXF files, shall be processed/converted and produced as single-page JPG image files and accompanied by a Concordance® Image formatted load file as described above. The native files shall be placed in a separate folder on the production media and linked by a hyperlink within the text load file.
- b. GIS data shall be produced in its native format and be accompanied by a viewer such that the mapping or other data can be reviewed in a manner that does not detract from its ability to be reasonably understood.
- c. Audio and video recordings shall be produced in native format and be accompanied by a viewer if such recordings do not play in a generic application (e.g., Windows Media Player).

### 17. Bates Number Convention

All images should be assigned Bates numbers before production to the government. Each Bates number shall be a standard length, include leading zeros in the number, and be unique for each produced page. The numbers should be endorsed on the actual images at a location that does not obliterate, conceal, or interfere with any information from the source document. Native files should be assigned a single Bates number for the entire file which will represent the native document in the Opticon/Concordance® Image Cross Reference file. The load file will include a reference to the native file path and utilize the NATIVELINK metadata field). The Bates number shall not exceed 30 characters in length and shall include leading zeros in the numeric portion. The Bates number shall be a unique number given sequentially (i.e., page one of document is PREFIX00000000001, page two of the same document is PREFIX00000000002) to each page (when assigned to an image) or to each document (when assigned to a native file). If the parties agree to a rolling production, the numbering convention shall remain consistent throughout the entire production. There shall be no spaces between the prefix and numeric value. If suffixes are required, please use “dot notation.” Below is a sample of dot notation:

|         | <u>Document #1</u>    | <u>Document #2</u>    |
|---------|-----------------------|-----------------------|
| Page #1 | PREFIX00000000001     | PREFIX00000000002     |
| Page #2 | PREFIX00000000001.002 | PREFIX00000000002.002 |
| Page #3 | PREFIX00000000001.003 | PREFIX00000000002.003 |

### 18. Other Production Formats

If other ESI or document production formats are required but are not included in these specifications (including, but not limited to, mobile devices, workplace collaboration sites (e.g. Teams, Slack), smart phones, social media, translated documents, audio files, non-Windows based documents and non-PC based documents), the producing party shall obtain written approval from the Government on the specific technical production specifications required prior to production.

### 19. Media Formats for Storage and Delivery of Production Data

Electronic documents and data shall be delivered on any of the following media:

- a. CD-ROMs and/or DVD-R (+/-) formatted to ISO/IEC 13346 and Universal Disk Format 1.02 specifications; Blu-ray.



- b. External hard drives (USB 3.0 or higher, formatted to NTFS format specifications) or flash drives.
- c. Government approved File Transfer Protocol (FTP) technologies.
- d. Storage media used to deliver ESI shall be appropriate to the size of the data in the production.
- e. Media should be labeled with the case name, production date, Bates range, and producing party.

## **20. Virus Protection and Security for Delivery of Production Data**

Production data shall be free of computer viruses. Any files found to include a virus shall be quarantined by the producing party and noted in a log to be provided to the government. Password protected or encrypted files or media shall be provided with corresponding passwords and specific decryption instructions. All encryption software shall be used with approval by and with the written consent of the government.

## **21. Compliance and Adherence to Generally Accepted Technical Standards**

Production shall be in conformance with standards and practices established by the National Institute of Standards and Technology (“NIST” at [www.nist.gov](http://www.nist.gov)), U.S. National Archives & Records Administration (“NARA” at [www.archives.gov](http://www.archives.gov)), American Records Management Association (“ARMA International” at [www.arma.org](http://www.arma.org)), American National Standards Institute (“ANSI” at [www.ansi.org](http://www.ansi.org)), International Organization for Standardization (“ISO” at [www.iso.org](http://www.iso.org)), and/or other U.S. Government or professional organizations.

## **22. Read Me Text File**

All deliverables shall include a “read me” text file at the root directory containing: Total number of records, total number of images/pages or files, mapping of fields to plainly identify field names, types, lengths, and formats. The file shall also indicate the field name to which images will be linked for viewing, date and time format, and confirmation that the number of files in load files matches the number of files produced.

## **23. Exception Report**

An exception report, in .csv format, shall be included, documenting any production anomalies during the collection, processing, and production phases. The report shall provide all available BEGDOC# or DOCID values and metadata listed in Section 3, including but not limited to file names and file paths for all affected files.

## **23. Transmittal Letter to Accompany Deliverables**

All deliverables should be accompanied by a transmittal letter including the production date, case name and number, producing party name, and Bates range produced. Technical instructions on how to decrypt media should be included in the transmittal letter but the password should be transmitted separately.



## PRIVACY ACT NOTICE FORM

The standard Privacy Act Notice is provided for all DoD IG Subpoenas and is generated by the DoD IG Subpoena Program Office.

### NOTICE PURSUANT TO PRIVACY ACT OF 1974

The Privacy Act of 1974 directs that persons, such as those individuals required by the Inspector General of the Department of Defense (DoD) to supply information in response to a subpoena, be informed of the following:

1. Authority for Solicitation of the Information:

The authority for requiring production of the information is set forth in the Inspector General Act of 1978, Public Law 95-452 and Public Law 97-252. Disclosure of information is mandatory.

2. Principal Uses of the Information:

The Inspector General's principal purpose in soliciting the information is to promote economy, efficiency, and effectiveness in the administration of the programs and operations of DoD and to prevent and detect fraud and abuse in such programs and operations.

3. Effect of Noncompliance:

Failure to comply with a subpoena may result in the Inspector General's requesting a court order for compliance. If such an order is obtained and you thereafter fail to supply the information, you may be subject to civil and/or criminal sanctions for contempt of court.

4. Routine Uses of the Information:

Information you give may be used and disseminated in the routine operation of DoD, including criminal, civil, and administrative proceedings. Routine uses include, but are not limited to, the following categories:

a. In any case in which there is an indication of a violation or a potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

b. In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local or foreign agency, or to an individual organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;



c. A record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practices;

d. A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings;

e. A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

f. A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;

g. A record may be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

h. A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of license, grant, or other benefit by the requesting agency to the extent that the information relates to the requesting agency's decision on the matter;

i. A record may be disseminated to the public, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than information such as a modus operandi.

#### 5. Freedom of Information Act:

The Freedom of Information Act (FOIA), Title 5, U.S.C., Section 552, and DoD rules pursuant thereto, generally provide for access by members of the public to governmental records, unless the requested records fall within specified exemptions. If you believe that one or more of the documents required under this subpoena should be considered exempt in whole or in part from public release under the FOIA, Title 5, U.S.C., Section 552, you must mark each document, which you believe exempt. In a letter accompanying the documents, you should cite all exemptions contained in the FOIA that you believe apply and the reasons for each. It is the policy of the Office of the Inspector General to seek to notify you in the event that it receives a request under the FOIA for records for which you have claimed exemption or in the event that legal proceedings are initiated against the Office of the Inspector General to obtain such records.



**CERTIFICATE OF COMPLIANCE (RECIPIENT / CUSTODIAN OF RECORDS) FORM**

The Certificate of Compliance form is provided to the recipient/custodian of records for completion when the records are provided to the Government. The form is generated by the DoD IG Subpoena Program Office.

**CERTIFICATE OF COMPLIANCE**

I, \_\_\_\_\_, of \_\_\_\_\_ of  
(Name) (Title)  
\_\_\_\_\_,  
(Company/Institution/Agency)

certify the records I provided (either) to Special Agent, \_\_\_\_\_,

or by certified mail accountability number \_\_\_\_\_, return receipt

requested, are accurate, complete, and in full compliance with the Department of Defense

Inspector General Duces Tecum number \_\_\_\_\_.  
(Unique Identification Number)

The following subpoenaed records are not provided. (If documents are withheld based on privilege, identify each document, specify its author and addressee, date, subject matter, all persons or entities to whom copies were furnished, and the basis of your claim of privilege.)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(Use attachment if necessary)

In accordance with, Title 28, United States Code, Section 1746, I certify under penalty of perjury the foregoing is true and correct.

\_\_\_\_\_  
(Signature of Respondent)

\_\_\_\_\_  
(Date)



### CERTIFICATE OF RETURN OF SERVICE

The Certificate of Return of Service is not provided to the subpoena recipient. The Certificate of Return of Service is to be completed by the requestor IMMEDIATELY AFTER SERVICE of the subpoena(s) or as soon as practicable. Email a copy to the completed Certificate of Return of Service to the DoD IG Subpoena Program Office at subpoena@dodig.mil IMMEDIATELY or NO LATER THAN the first business day after service. Receipt of the completed Certificate of Return of Service by this office closes the Request For Subpoena process. These actions are not related to the production of documents by the subpoena recipient(s).

### CERTIFICATE OF RETURN OF SERVICE

I HEREBY CERTIFY that on \_\_\_\_\_, 2023  
(Date Subpoena Packet Received)

I received the attached subpoena. I further certify that on \_\_\_\_\_, 2023  
(Date Recipient Served)

at or about \_\_\_\_\_ m. at \_\_\_\_\_, I personally  
(Time of Service) (Location of Service\*)

served the subpoena upon \_\_\_\_\_.  
(Name and Position/Title to whom was served)

Serving Agent/Investigator: \_\_\_\_\_  
(Name and Position/Title of who served the subpoena)

NOTE: Please complete as soon as possible, but no later than five business days after serving the subpoena recipient and email the completed certificate to DoD IG Subpoena Program Office at subpoena@dodig.mil. The Certificate of Return of Service is to be completed by the serving Agent/Investigator at the time the subpoena is served. This lets our office know you have served the subpoena. It does not pertain to the return of documents.

\*If service was completed by certified or registered mail, list associated number for location of service. If service was completed by email, fax, or portal, list the associated information for location of service.

UNIQUE IDENTIFICATION NUMBER: 2023XXXX-XXXXX



**MEMORANDUM GRANTING REQUEST FOR EXTENSION ON DOD IG SUBPOENA COMPLIANCE DATE**

This memorandum is not required; however, it is recommended to document all extensions in writing. Extensions do not need to be coordinated with the DoD IG Subpoena Program Office. This memorandum is only a recommendation and is provided as an example.

**Agency Letterhead**

**FROM:** Special Agent XXXXX

**TO:** Mr. XXXXX

Legal Representative for XXXXX Corporation  
XX XXXXXXXXXX XXXXX  
XXXXXXXX, XX XXXXX

**SUBJECT:** Request for Subpoena Compliance – XXXXX Corporation

On February 10, 2023, Special Agent XXXXX spoke with Mr. XXXXX regarding XXXXX Corporation's request for a 60 day extension to the original subpoena compliance date of January 31, 2023, for DoD IG Subpoena Unique Identification Number: 2023XXXX-XXXXX, which was served on January 1, 2023.

This Memorandum serves as an understanding between Mr. XXXXX and XXXXX, that a good faith effort will be made by XXXXX Corporation to produce requested documents, initially on a prioritization basis based on concurrence with Special Agent XXXXX. The production of records will be on a rolling basis and will commence no later than March 15, 2023. Upon completion of providing all documents requested in the subpoena, a signed Certificate of Compliance (provided when subpoena was served) will be signed and submitted to OSI PF Detachment X. If there are any questions or concerns, please contact Special Agent XXXXX at (XXX) XXX-XXXX or via email at XXXXX@us.mail.mil. Request that you sign and date this memorandum below and return to Special Agent XXXXX.

XXXXX XXXXX, Special Agent  
OSI PF Detachment X

**ACKNOWLEDGEMENT:**

As an agent of XXXXX Corporation, I hereby acknowledge that XXXXX Corporation is being granted an extension of time which to comply with the above referenced subpoena in accordance with the terms and conditions set forth above.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)





## APPENDIX D – INSTRUCTIONS CONCERNING DOD IG SUBPOENAS COVERED BY THE RFPA

The Right to Financial Privacy Act (hereafter, the “Act”)<sup>1</sup> affects subpoenas served on a “financial institution” for records concerning a “customer” of that financial institution as defined by the Act. “Financial institution” basically includes traditional banks and savings and loan institutions, credit unions, and credit card issuing institutions. Investment firms, for example, would not be financial institutions under the Act unless they issue credit cards or offer draft accounts. “Customer” includes an individual or a partnership of five or fewer partners. Larger partnerships and corporations (regardless of the number of corporate owners) are not “customers” under the Act.

The purpose of the Act is to provide added privacy to a customer’s financial records. Concerning subpoenas for financial records, the Act requires that a customer be notified of the Government’s intention to obtain financial records prior to the actual service of a subpoena. Upon receiving such notification, a customer may then file a motion in Federal district court to challenge the subpoena. To prevail, the customer must be able to show that the records sought are either not relevant to your investigation, are unduly broad in scope, or that the investigation itself is either unauthorized or baseless. Accordingly, most challenges are unsuccessful because subpoena requests are screened for the same attributes before they are approved.

### SUBPOENA REQUEST PACKAGES

In addition to the standard documents (request memorandum, custodian letter, Privacy Act notice, and Certificate of Compliance) included in a subpoena request, subpoena requests for financial records subject to the Act must also include:

- Customer notice letter
- Statement of customer rights under the Right to Financial Privacy Act
- Instructions for completing and filing a motion and sworn statement
- Blank motion form
- Blank statement form
- Certificate of Service<sup>2</sup>
- Agent Certificate of Compliance<sup>3</sup>

<sup>1</sup>12 U.S.C. § 3401 et seq.

<sup>2</sup>Customers use this form to notify the investigator that the customer is filing, or has filed a motion with a particular court. Although the form is provided to the customer, there is no legal requirement for the customer to so notify the investigator. Therefore, investigators may not assume that a motion has not been filed simply because the investigator did not receive a certificate of service.

<sup>3</sup>Form completed by the investigator and provided to the financial institution certifying that the investigator has complied with the requirements of the Right to Financial Privacy Act, i.e., that the investigator has properly notified the customer and waited the requisite 10 or 14 days prior to taking custody of the subpoenaed documents.





Be sure to include, in your customer notification letter, the address and phone number for each Federal district court (clerk's office) where the customer may file a motion to challenge. Generally, that would include the court having jurisdiction over the customer's place of residence, the court having jurisdiction over the location of the bank being served the subpoena, and the court for the Eastern District of Virginia (location of the DoD Inspector General).<sup>4</sup> In overseas cases, include the court having jurisdiction in the geographical area covering the customer's home of record and/or last place of residence. The court for the District of Columbia also hears cases involving extraterritorial jurisdiction. A good resource for locating district court offices is at <https://www.uscourts.gov/>.

**REQUIRED INVESTIGATOR ACTIONS FOLLOWING RECEIPT OF SIGNED SUBPOENAS FOR FINANCIAL RECORDS AFFECTED BY THE ACT**

1. Serve notice on the customer by providing:
  - a. Notice to customer
  - b. Statement of customer rights under the Right to Financial Privacy Act
  - c. Copy of the subpoena and appendix (if there is an appendix)
  - d. Instructions for completing and filing a motion and sworn statement
  - e. Blank motion form
  - f. Blank statement form
  - g. Certificate of Service
2. Customer can be notified in person or via certified mail (return receipt).
3. Wait for a period of 10 calendar days following in-person notification and 14 calendar days following notification by mail.<sup>5</sup>

<sup>4</sup>401 Courthouse Square, Alexandria, VA 22320 (703) 299-2100.

<sup>5</sup>Under Rule 6 of the Federal Rules of Civil Procedure, in computing the waiting time, the day that notice is made is not counted in the total. Additionally, if the 10th or 14th day is Saturday, Sunday, or legal holiday, or the office of the clerk of court is not accessible that day due to inclement weather, the final day will be the next day that is not one of the aforementioned days. "Legal holiday" includes New Year's Day, Birthday of Martin Luther King, Jr., Washington's Birthday, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, Christmas Day, and any other day appointed as a holiday by the President, the Congress of the United States, or by the state in which the district court is located.



4. Contact the clerks of court in all potential jurisdictions. Unless there is already an open criminal or civil case with the court, the motion you are looking for will likely be treated as a miscellaneous civil filing.

5. If a motion to challenge has not been filed, serve the subpoena on the financial institution and provide them with your certificate of compliance. If a motion to challenge has been filed, obtain as much information about it as possible from the court clerk and contact the DoD IG Subpoena Program Manager and your Assistant U.S. Attorney/military Staff Judge Advocate. The court may rule with no further action required on your part, or the Government may need to file a countermotion. You may not serve the subpoena until the court has denied the customer's motion.



## APPENDIX E – SAMPLE PACKET FOR FINANCIAL DOD IG SUBPOENAS

### CUSTOMER NOTICE LETTER (SUBJECT)

The customer notice is prepared by the DoD IG Subpoena Program Office for all subpoenas requesting customers' financial records from financial institutions. It provides information to the customer on what records are being sought, the criminal statutes or UCMJ Articles the subject is suspected of violating, how an objection to the release of the records can be filed, and in what court(s) the objection can be filed. As attachments, the customer notice provides copies of the following: Copy of Subpoena and Appendix (if there is an appendix); Statement of Customer Rights under the RFPA; Instructions for completing motion and sworn statement; Blank Motion form; Blank statement form; and Certificate of Service. The customer is directed to send a copy of his motion and statement to the DoD IG Subpoena Program Office.

### (Agency Letterhead)

### NOTICE TO CUSTOMER

MSgt John Q. Public  
1234 Main Street  
Jackson, MS 39201

Dear MSgt Public:

Records or information concerning your transactions held by the financial institution named in the attached subpoena are being sought by the Office of the Inspector General, Department of Defense, in accordance with the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ Section 3401*et seq.*, for the following purpose(s):

**(Example: “To refute or support allegations that you submitted false statements and false claims pertaining to the ABC base services contract from on or about July 4, 2007 through January 1, 2009, that appears to be in violation of 18 United States Code (U.S.C.) § 287, False Claims, and 18 U.S.C. § 1001, False Statement.”)**

If you desire that such records or information not be made available, you must:

(1) Fill out the accompanying motion paper and sworn statement (as indicated by the instructions beneath each blank space) or write one of your own, state that you are the customer whose records are being requested by the Government, and give the reasons you believe that the records are not relevant to the legitimate law enforcement inquiry stated in this notice or any other legal basis for objecting to the release of the records.



(2) File the motion and sworn statement by mailing or delivering them to the clerk of any one of the following United States District Courts:

Virginia Eastern District Court  
Albert V. Bryan United States Courthouse, 2<sup>nd</sup> Floor  
401 Courthouse Square  
Alexandria, VA 22314  
(703) 299-2100

This information will be listed on each letter as it is the District Court having jurisdiction over the DoD OIG's location.

Mississippi Southern District Court  
501 East Court Street  
Jackson, MS 39201  
(601) 608-4000

This information will be for the District Court having jurisdiction over the customer's place of residence.

Indiana Southern District Court  
Birch Bayh Federal Building and U.S. Courthouse  
46 East Ohio Street, Room 105  
Indianapolis, IN 46204  
(317) 229-3700

This information will be for the District Court having jurisdiction over the location of the bank being served the subpoena.

(It would simplify the proceeding if you would include with your motion and sworn statement a copy of the attached subpoena, as well as a copy of this notice.)

(3) Serve the Government authority requesting the records by mailing (by registered or certified mail) or by delivering a copy of your motion and sworn statement to: **Inspector General of the Department of Defense, Office of General Counsel, c/o DoD IG Subpoena Program, 4800 Mark Center Drive, Suite 15K26, Alexandria, VA 22350-1500.**

(4) Be prepared to come to court and present your position in further detail.

(5) You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of ten days from the date of service or fourteen days from the date of mailing of this notice, the records or information requested therein may be made available. These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer.



Sincerely,

JOHN Q. SMITH, Special Agent  
Director of Operations

Enclosures:  
Subpoena Duces Tecum  
Appendix A  
Statement of Customer Rights under the  
Right to Financial Privacy Act of 1978  
Instructions for Completing and Filing  
Motion and Sworn Statement  
Motion Form  
Sworn Statement Form  
Certificate of Service



## STATEMENT OF CUSTOMER RIGHTS FORM

The Statement of Customer Rights Form provides a concise explanation of customer rights under the RFPA.

### STATEMENT OF CUSTOMER RIGHTS UNDER THE FINANCIAL PRIVACY ACT OF 1978

Federal law protects the privacy of your financial records. Before banks, savings and loan associations, credit unions, credit card issuers, or other financial institutions may give financial information about you to a federal agency, certain procedures must be followed.

**CONSENT TO FINANCIAL RECORDS:** You may be asked to consent to the financial institution making your financial records available to the Government. You may withhold your consent, and your consent is not required as a condition of doing business with any financial institution. If you give your consent, it can be revoked in writing at any time before your records are disclosed. Furthermore, any consent you give is effective for only three months, and your financial institution must keep a record of the instances in which it discloses your financial information.

**WITHOUT YOUR CONSENT:** Without your consent, a federal agency that wants to see your financial records may do so ordinarily only by means of a lawful subpoena, summons, formal written request, or search warrant for that purpose. Generally, the federal agency must give you advance notice of its request for your records explaining why the information is being sought and telling you how to object in court. The federal agency must also send you copies of court documents to be prepared by you with instructions for filling them out. While these procedures will be kept as simple as possible, you may want to consult an attorney before making a challenge to a federal agency's request.

**EXCEPTIONS:** In some circumstances, a federal agency may obtain financial information about you without advance notice or your consent. In most of these cases, the federal agency will be required to go to court for permission to obtain your records without giving you advance notice. In these instances, the court will make the Government show that its investigation and request for your records are proper. When the reason for the delay of notice no longer exists, you will usually be notified that your records were obtained.

**TRANSFER OF INFORMATION:** Generally, a federal agency that obtains your financial records is prohibited from transferring them to another federal agency unless it certifies that the transfer is proper and sends a notice to you that your records have been sent to another agency.

**PENALTIES:** If the federal agency or financial institution violates the Right to Financial Privacy Act, you may sue for damages or seek compliance with the law. If you win, you may be repaid your attorney's fee and other costs.



ADDITIONAL INFORMATION: If you have any questions about your rights under this law, or about how to consent to release your financial records, please call the official whose name and telephone number appear below:

---

Special Agent John Q. Doe  
Office of Special Investigations Detachment 1234  
1234 Air Force Way  
Any Air Force Base, VA 12345  
Phone: (202) 123-4567  
Email: john.doe@us.af.mil



### **INSTRUCTIONS FOR COMPLETING AND FILING MOTION AND SWORN STATEMENT FORMS**

This form provides the customer whose records are being subpoenaed the information needed to file an objection to the release of the records.

## **INSTRUCTIONS FOR COMPLETING AND FILING THE ATTACHED MOTION AND SWORN STATEMENT**

1. Except where signatures are required, the indicated information should be either typed or printed legibly in ink in the spaces provided on the attached motion and sworn statement forms. The information required for each space is described in parentheses under each space to be completed.
2. The most important part of your motion is the space on the “sworn statement” form where you must state your reasons for believing that the financial records sought are not relevant to the legitimate law enforcement inquiry stated in the attached notice. You may also challenge the government's access to the financial records if there has not been substantial compliance with the Right to Financial Privacy Act or for any other reasons allowed under the law. You should state the facts that are the basis for your challenge as specifically as you can.
3. To file your motion with the court, either mail or deliver the original and the proper number of copies, as well as any required filing fee, to the Clerk of the Court. The filing fee can be paid with cash, certified check, or money order. You are required to check with the Clerk of the Court for the district in which you intend to file to ascertain the correct filing fee and correct number of copies required for filing, as well as to ascertain any other local rules of court that may exist.
4. One copy of your challenge papers (motion and sworn statement) and Certificate of Service must be delivered or mailed (by registered or certified mail) to the government official whose name appears in item 3 of the customer notification letter.
5. If you have further questions, contact the government official whose name and telephone appear on the Customer Notice.





**BLANK MOTION FORM**

This form provides the customer whose records are being subpoenaed the form needed to file an objection to the release of the records being subpoenaed.

**CUSTOMER'S MOTION TO CHALLENGE GOVERNMENT'S ACCESS  
TO FINANCIAL RECORDS IN THE UNITED STATES  
DISTRICT COURT**

FOR THE \_\_\_\_\_ DISTRICT OF \_\_\_\_\_  
(Name of District) (State in Which Court is Located)

|                       |   |                            |
|-----------------------|---|----------------------------|
| _____                 | ) | Miscellaneous No.          |
| (Your Name)           | ) | (Will be filled in by      |
|                       | ) | Court Clerk)               |
| Movant                | ) |                            |
| V.                    | ) |                            |
| Department of Defense | ) | MOTION FOR ORDER PURSUANT  |
|                       | ) | TO CUSTOMER CHALLENGE      |
| Respondent            | ) | PROVISIONS OF THE RIGHT TO |
|                       | ) | FINANCIAL PRIVACY ACT      |
|                       | ) | OF 1978.                   |

\_\_\_\_\_ hereby move this Court pursuant to  
(Your Name)

Section 3410 of the Right to Financial Privacy Act of 1978, 12 United States Code 3410, et seq. for an order preventing the Government from obtaining access to my financial records. The agency seeking access is the Department of Defense.

My financial records are held by \_\_\_\_\_.  
(Name of Institution)

In support of this motion, the Court is respectfully referred to my sworn statement filed with this motion.

Respectfully submitted,

\_\_\_\_\_  
(Your Signature)

\_\_\_\_\_  
(Your Address)

\_\_\_\_\_  
(Your Telephone Number)

Right to Financial Privacy Act of 1978, Title 12 United States Code, Section 3410



**BLANK STATEMENT FORM (AFFIDAVIT)**

This form provides the customer whose records are being subpoenaed the form needed to submit a sworn statement challenging the release of the records being subpoenaed.

**CUSTOMER'S SWORN STATEMENT FOR FILING A CHALLENGE  
IN THE UNITED STATES DISTRICT COURT**

FOR THE \_\_\_\_\_ DISTRICT OF \_\_\_\_\_  
(Name of District) (State in Which Court is Located)

|                       |   |                                    |
|-----------------------|---|------------------------------------|
| _____                 | ) | Miscellaneous No. _____            |
| (Customer's Name)     | ) | (Will be filled in by Court Clerk) |
|                       | ) |                                    |
| Movant                | ) |                                    |
|                       | ) | <u>SWORN STATEMENT OF MOVANT</u>   |
| V.                    | ) |                                    |
|                       | ) |                                    |
| Department of Defense | ) | FINANCIAL PRIVACY ACT OF 1978      |
|                       | ) |                                    |
| Respondent            | ) |                                    |

I, \_\_\_\_\_, (am presently/was previously) a customer of  
(Customer's Name) (Show One)

\_\_\_\_\_, and I am the customer whose records are being  
(Name of Financial Institution)  
requested by the Government.

The financial records sought by the Department of Defense are not relevant to the legitimate law enforcement inquiry  
stated in the Customer Notice that was sent to me because \_\_\_\_\_

\_\_\_\_\_, or should not be disclosed because there  
has not been substantial compliance with the Right to Financial Privacy Act of 1978 in that \_\_\_\_\_  
or should not be disclosed on the following other legal basis: \_\_\_\_\_

I declare under penalty of perjury that the foregoing is true and correct.

\_\_\_\_\_, \_\_\_\_\_  
(Month) (Day) (Year) (Customer's Signature)

Right to Financial Privacy Act of 1978, Title 12 United States Code, Section 3410



**CERTIFICATE OF SERVICE FORM (CUSTOMER NOTIFICATION)**

This form provides the customer whose records are being subpoenaed a means of notifying the DoD IG Subpoena Program Director of a challenge to the subpoena.

**CERTIFICATE OF SERVICE**

I have mailed or delivered a copy of this motion and the attached sworn statement to

\_\_\_\_\_ on \_\_\_\_\_, \_\_\_\_\_.  
(name of the office listed in item 2 of customer notice) (month, day) (year)

\_\_\_\_\_  
(your signature)

Right to Financial Privacy Act of 1978, Title 12 United States Code, Section 3410



**AGENT'S CERTIFICATE OF COMPLIANCE  
(AGENT PROVIDES TO FINANCIAL INSTITUTION)**

The Agent's Certificate of Compliance is prepared by the DoD IG Subpoena Program Office for all subpoenas requesting customers' financial records from financial institutions. This form is signed by the requestor and certifies to the financial institution that the requestor complied with all of the requirements of the RFPA.

**(Agency Letterhead)**

Special Agent John Q. Doe  
Department of the Army Criminal Investigation Division  
Fort Base Resident Agency  
1234 Army Way  
Fort Base, VA 12345

Custodian of Records  
*(Name of Financial Institution)*  
*(Physical Address of Financial Institution)*  
*(City, State, Zip Code of Financial Institution)*  
*(ATTN: Point of Contact at Financial Institution if known)*

**CERTIFICATE OF COMPLIANCE WITH THE RIGHT TO FINANCIAL  
PRIVACY ACT**

I certify, pursuant to Section 3403(b) of the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 et seq., that the applicable provisions of that statute have been complied with as to the Department of Defense (DoD) Inspector General subpoena number

\_\_\_\_\_ presented on \_\_\_\_\_, \_\_\_\_\_, for the financial records of \_\_\_\_\_.

Pursuant to Section 3417(c) of the Right to Financial Privacy Act of 1978, good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records.

JOHN Q. DOE, Special Agent  
Fort Base Resident Agency, Fort Base, VA



## APPENDIX F – RESOURCES

### 1. Commercial and Government Entity (CAGE)

The Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) website provides a standalone solution to search for foreign and domestic entity's CAGE information. Site capabilities include:

- Search for CAGE code information at CAGE Search & Inquiry (CSI)
- Access to forms required to support transactions
- Frequently Asked Questions
- Request a New CAGE code not associated with a System for Award Management (SAM) registration
- Providing update information for an existing CAGE code not associated with a SAM registration
- Scheduled maintenance notifications
- Upcoming changes

**Website Address:** <https://cage.dla.mil/>

### 2. U.S. District Court Links

The site provides information on U.S. District Courts (and Bankruptcy Courts) such as address, phone number, and website. The site is searchable by state, city, county, circuit, zip code, and area code.

**Website Address:** <https://www.uscourts.gov/>

### 3. Internet Service Provider (ISP) Listing

SEARCH.org is an online resource for justice and public safety officials. It contains listings of Internet Service Providers (ISPs), contacts at legal departments for law enforcement service of subpoenas, court orders, and search warrants.

**Website Address:** <https://www.search.org/resources/isp-list/>

### 4. System for Award Management (SAM)

The System for Award Management (SAM) is a U.S. government website that allows businesses to register to do business with the U.S. government and includes detailed information on the business's entity registration and any exclusion records.



**Website Address:** <https://sam.gov/SAM/pages/public/searchRecords/search.jsf>

## 5. Fraud Detection Resources

This website provides excellent information on audit risk factors, audit planning, referring matters to appropriate investigative organizations and includes information such as general fraud scenarios and indicators; fraud red flags and indicators; and fraud detection resources.

**Website:** <https://www.dodig.mil/Resources/Fraud-Detection-Resources/>

## 6. FoneFinder

FoneFinder website provides an online resource for determining the name of the telephone (landline or mobile cellular) carrier for the number provided.

**Website Address:** <http://www.fonefinder.net/>

## 7. IP Location

IP Location website provides an online resource for determining the geographic location and ISP for the targeted IP address.

**Website Address:** <https://www.iplocation.net/>



## APPENDIX G – ADMINISTRATIVE REMINDERS

Include the cell phone number of the case agent.

There must be a physical address for the return of service, i.e., the DCIO office address.

When listing businesses and corporations, be sure to use the complete legal corporate name.

When providing addresses, please use the physical address as PO Boxes are not typically acceptable.

Zip codes must match the physical address.

If previous DoD IG Subpoenas have been issued, identify the subpoena recipient and the DoD IG Subpoena Unique Identification Number. If the request is for the same recipient, explain how these requested records differ from those previously obtained/requested. [Block 6 of Request Memorandum]

When listing the statutes, provide the full Uniform Code of Military Justice (UCMJ) or United States Code Section and Title, i.e., UCMJ Article 132, Frauds against the U.S. Government. Make sure the violation/crime falls within the Statute of Limitations. [Block 7 of Request Memorandum]

Be sure to include the Subject's full information such as rank/grade and status (Active, Guard, Reserve) [Block 8 of Request Memorandum]

When providing the Summary of Investigation, provide sufficient details for the DoD IG Subpoena Program Office to make a determination of whether the subpoena request is justified. [Block 9 of Request Memorandum]

Provide the name and title of the prosecutor (SJA, AUSA), their contact information, the date of coordination, and their concurrence with requesting a subpoena in this matter. [Block 10 of Request Memorandum]

When describing records and dates of required records, focus on the DoD nexus and why the documents and the dates are relevant to the investigation.

We require all request documents be submitted in Microsoft Word® format. Signatures are not required. If your agency requires signed PDF documents for submission of your request, please submit identical Microsoft Word® documents without digital signature.

Please remember to change the letterhead to your office's letterhead and do not delete any of the questions or change the format of the template. If the question is not applicable to your request, you may answer with "N/A" or "No", whichever is appropriate.



## APPENDIX H – INVESTIGATIVE PLANNING CONSIDERATIONS

### 1. Early Investigative Planning Stage:

- Early in your investigation, identify and list the types of records/documents that may be needed to substantiate or refute the allegation and support your investigative efforts.
- Some documents may be readily available without a subpoena, while others may require the issuance of a DoD IG Subpoena.
- Always check with the DoD IG Subpoena Program Office if you have questions on whether the documents can be obtained via a DoD IG Subpoena.

### 2. Considerations:

- Identify and determine the probative value of the records/documents requested (for example, how could obtaining cell phone records assist in determining if an individual made a call to someone from inside their residence?)
- If video images (surveillance footage) or access logs (hotel room, etc.) are needed, determine the entity's retention period, release policy, and any required specific descriptive details needed to be incorporated into the subpoena.
- If cellular phone records are needed, verify the number and carrier. The same also goes for financial institutions and bank account numbers.

If records are needed from a financial institution, in accordance with the Right to Financial Privacy Act (RFPA), the customer (Subject) must be given notice and the opportunity to file a motion to challenge/quash subpoena. In other words, they are going to know they are under investigation. If alerting the Subject that they are under investigation could cause an issue, such as the destruction of evidence, etc., you may want to give consideration to delaying any request for financial records until a more appropriate time when notification of the Subject does not pose a problem.