Department of Defense
Office of Inspector General

DOD INSPECTOR GENERAL SUBPOENA REFERENCE GUIDE

DoD Office of Inspector General
Investigative Policy and Oversight
Policy and Programs Directorate
DoD IG Subpoena Program Office

FEBRUARY 2017

FOREWARD

Department of Defense (DoD) Inspector General (IG) subpoenas are an essential and very valuable tool for all field agents. In many cases, DoD IG subpoenas are the only means of compelling the production of key records and documents in fraud and criminal investigations. The advantage of using DoD IG subpoenas is that they can be used in criminal, civil, and administrative actions.

The DoD IG Subpoena Program Office is dedicated to ensuring the field is provided with superior support and assistance in the timely and efficient processing of requests for DoD IG subpoenas

This reference guide was developed to assist you in the preparation of your requests for DoD IG subpoenas and to answer the most frequently asked questions. If you are planning on submitting your first request for a DoD IG subpoena, have not submitted a DoD IG subpoena request in a while, or are planning on submitting a request for a DoD IG subpoena in connection with a unique set of facts, we suggest that you call our office first so we can discuss the aspects of your investigation and your subpoena request. This will enable us to answer any questions you may have, provide initial guidance on the submission of your request and in some cases provide a sample template to use during the preparation of your subpoena request.

CONTACT INFORMATION

Mailing Address:

Inspector General, Department of Defense
Assistant Inspector General
Investigative Policy and Oversight
ATTN: DoD IG Subpoena Program Office
4800 Mark Center Drive, Suite 11H25, West Tower
Alexandria, VA 22350-1500

E-Mail Address: subpoena@dodig.mil

Website Address: http://www.dodig.mil/programs/subpoena/index.html

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

REFERENCE INDEX

REFERENCE INDEX

GENERAL INFORMATION

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-1	**Eligibility to Request a DoD IG Subpoena**	Any agent of a Defense Criminal Investigative Organization (DCIO) may request a DoD IG subpoena. This includes the Defense Criminal Investigative Service (DCIS), The U.S. Army Criminal Investigation Command (USACIDC), the Naval Criminal Investigative Service (NCIS), and the Air Force Office of Special Investigations (AFOSI). Requests from other DoD investigators, law enforcement officials, and Service Inspectors General will be reviewed on a case-by-case basis. Military police organizations should process their requests through USACID, NCIS, or AFOSI. Requests will also be processed for internal DoD OIG components (AI, SPO, Audit, etc.). DoD OIG Components requiring a DoD IG subpoena should contact the DoD IG Subpoena Program Office for assistance.

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-2	**Benefits of Using DoD IG Subpoenas**	**1.** An IG subpoena is enforceable. If the recipient fails to comply, a court order may be sought to compel compliance. **2.** An IG subpoena is administrative. Unlike a grand jury subpoena, an IG subpoena can be used to support civil and administrative remedies, as well as criminal prosecution. **3.** An IG subpoena is not subject to the secrecy requirements associated with a grand jury subpoena.
1-3	**Requesting a DoD IG Subpoena**	DCIOs and others send DoD IG subpoena requests and associated supporting documentation by e-mail to the DoD IG Subpoena Program Office at **subpoena@dodig.mil**, or they may send their requests to the specific case officer in the DoD IG Subpoena Program Office.

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-4	**Means of Serving the Subpoena**	DoD IG subpoenas may be served in person by a DCIO special agent or by registered or certified mail with a return receipt. Subpoenas may also be served via fax or e-mail, provided the recipient agrees in advance. Discuss the service of subpoenas via fax or e-mail with the recipient to ensure this method is considered an acceptable method of service for legal documents. Subpoenas should be served as soon as practical as the recipient must be provided at least 30 days to comply.
1-5	**Serving DoD IG Subpoena to Recipient**	The Custodian Cover Letter to Subpoena Recipient, Privacy Act Notice, and a copy of the front of the DoD IG Subpoena with Appendix A (if applicable) must be served. Complete the Certificate of Service on the reverse side of the DoD IG subpoena and fax or e-mail a scanned copy to the DoD IG Subpoena Program Office. The original DoD IG subpoena should be placed in the case file for retention with other case-related documents.

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-6	**Request by Recipient for Additional Time for Compliance**	The subpoena should be served as soon as the agent receives the signed copy from the DoD IG Subpoena Program Office. If you believe the recipient is making a good faith effort to compile the requested records and simply needs more time, you may grant a reasonable extension to the due date. Get all such time extensions in writing. If it begins to appear like the recipient does not intend to properly comply, contact the DoD IG Subpoena Program Office. (See page 116.)

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-7	**Delivery of Subpoenaed Records to Case Agent**	Although the subpoena recipient should deliver the records in person, it is acceptable to allow the recipient to mail the requested records. The manner of delivery should be addressed in the subpoena cover letter and, if required, discussed with the recipient. Make sure you have the recipient sign a Certificate of Compliance attesting that all requested documents were provided.
1-8	**Special Handling for Subpoenas Deemed Urgent and Requiring to be Expedited**	The DoD IG Subpoena Program Office strives to prioritize and handle all subpoena requests as expeditiously as possible. However, there are instances that may dictate that the request be expedited with special handling. In those instances, the field agent should explain the rationale for requesting that the subpoena be expedited and receive special handling. Approval for special handling and the expedition of a DoD IG subpoena is based on the sensitivity and level of impact of the investigation.

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-9	**Forwarding of a Signed Subpoena and Associated Documents to the Field Agent**	All subpoenas are digitally signed and forwarded along with all other associated documents to the field agent in Adobe pdf format. Signed subpoenas cannot be sent to the Assistant United States Attorney (AUSA) office. They must be forwarded to the case agent's address, because the case agent is the agent of the DoD IG in connection with service of the subpoena.

GENERAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
1-10	Circumstances When a DoD IG Subpoena Would Not Be Appropriate	There are specific circumstances when a DoD IG subpoena would not be appropriate or approved, unless an exception to policy is granted by Office of General Counsel (OGC). These circumstances include: ▪ Records already in the possession of the U.S. Government, ▪ State, county and local Government unless it is stated that a subpoena is required, ▪ Records obtained via search warrant or grand jury subpoena, ▪ Credit Bureau information, ▪ Contents of communications, ▪ Bad check case [minimum of $1,000 loss to the Government (DoD)], ▪ Recipient is a member of the news media (special considerations), ▪ Preliminary inquiries (substantive cases only), ▪ Records related to loss of personal property, and ▪ Recipient is an attorney and the subpoena seeks documentation regarding the attorney-client relationship. There must be a monetary loss to the Government (DoD) or impact a DoD program or operation.

FINANCIAL INFORMATION

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-1	**Right to Financial Privacy Act (RFPA)**	The Right to Financial Privacy Act (RFPA), Sections 3401-3422, Title 12, United States Code (12 U.S.C. § 3401-3422), 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**	Any office of a bank, savings bank, credit card issuer, 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**	An 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**	Any person or authorized representative of that person who used or is using 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**	An 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**	If your subpoena is for records from a financial institution, you cannot serve the subpoena until you have met the customer notification requirements contained in the RFPA. Serve the notification documents to the account holder and wait ten (10) days if you notified them in person, or fourteen (14) days if you notified them via registered or certified mail with a return receipt. Regardless of whether the account holder sent you or the DoD IG Subpoena Program Office a certificate of service, you must check with the applicable clerks of court to determine if the account holder filed a motion to challenge the subpoena. The U.S. district courts should include the Eastern District of Virginia (location of DoD IG), the district court where the financial institution is located, and the district court where the customer resides. **[Please see U.S. District Court link in Resources Section, Page 75]** 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 Office immediately. You may not serve the subpoena on the financial institution until the court has denied the customer's motion. 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 subpoena on the financial institution along with a certificate attesting that you have complied with all RFPA requirements (Certificate of Compliance).

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-7	**Transfer of Financial Information to Another Federal Agency**	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 of any transfer, serve or mail 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, a copy of the certification and 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 [12 U.S.C. § 3401 et seq.] 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 [5 U.S.C. § 552a].

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-8	**Transfer of Financial Information to Other Agencies**	Transfer restrictions do not apply to intradepartmental transfers (e.g., AFOSI may transfer financial records to USACIDC 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 criminal law, and their use only for criminal investigative or prosecutive purposes. This precludes the transfer of records obtained under RFPA to the Fraud Section, Civil Division.

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-9	**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.

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-10	**Obtaining Basic Identifying Bank Account Information**	A subpoena is required to obtain basic financial account identifying information such as name of customer, account number, addresses, and type of account. The request for basic financial account identifying date must be associated with either a specific financial transaction or a class of financial transactions. 12 U.S.C. § 3413(g)
2-11	**Requests for Reimbursement of Costs Associated with DoD IG Subpoena Compliance**	The RFPA provides for the reimbursement to financial institutions for their research and copy costs. Rates are established in the Code of Federal Regulations (CFR). 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 IG.

FINANCIAL INFORMATION

NO.	TOPIC	COMMENT
2-12	**Handling Motions to Challenge and Quash a DoD IG Subpoena under the RFPA**	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. 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 IG's interest in obtaining the customer's financial records. OGC has only ten (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 taskings from OGC on the part of the case agent.

ELECTRONIC DATA

ELECTRONIC DATA		
NO.	**TOPIC**	**COMMENT**
3-1	**Authority to Subpoena Information from Internet Service Providers**	The Electronic Communication Privacy Act (ECPA), 18 U.S.C. §2701 et seq., establishes provisions for access, use, disclosure, interception, and privacy protections of electronic communications. Whenever agents seek stored e-mail, account records, or subscriber information from a network service provider, you must comply with the ECPA.
3-2	**Definition of Electronic Communications**	According to the ECPA, 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, photoelectronic or photooptical 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. The ECPA prohibits an electronic communications provider from producing contents of electronic communications, even pursuant to subpoena or court order, except in limited circumstances.

ELECTRONIC DATA		
NO.	**TOPIC**	**COMMENT**
3-3	**Disclosure of Basic Subscriber Information**	The ECPA allows for the disclosure of basic subscriber information with a subpoena. This information includes: ▪ Names(s); ▪ Address(es); ▪ Local and long distance telephone connection records or records of session times and durations; ▪ Length of service (including start date) and types of service used; ▪ Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and ▪ Means and source of payment for such service (including any credit card or bank account number). 18 U.S.C. §2703(c)(2)
3-4	**Disclosure of Other Information Pertaining to a Customer or Subscriber**	The ECPA 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. In order to obtain transactional information, a search warrant is required. U.S. v. Warshak

ELECTRONIC DATA		
NO.	**TOPIC**	**COMMENT**
3-5	**Disclosure of Electronic Communications Contents (less than 180 Days)**	The ECPA divides providers covered by the statute into "providers of electronic communication service" and "providers of remote computing service." A governmental entity may require the provider of electronic communication service to disclose the contents of a wire or electronic communication, that are in electronic storage in an electronic communications system under 180 days, only pursuant to a search warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent state warrant. U.S. v. Warshak
3-6	**Restrictions on Obtaining Electronic Communications (less than 180 Days)**	On December 14, 2010, the Sixth Circuit decided U.S. v. Warshak, 2010 WL 5071766 (6th Cir.) This decision has major implications for how DoD IG issues subpoenas. The Sixth Circuit held that the use of a 2703(d) order or subpoena (under the Electronic Communications Privacy Act) to compel disclosure of e-mail content from a commercial Internet Service Provider (ISP) violated the Fourth Amendment. 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.

ELECTRONIC DATA		
NO.	**TOPIC**	**COMMENT**
3-6	**Restrictions on Obtaining Electronic Communications (more than 180 Days)**	In the past, field agents could obtain basic subscriber information and with customer notice, could also obtain the contents of any wire or electronic communications held by a provider of remote computer services or that had been held in storage for more than 180 days. What this now means is that the DoD IG will not be issuing subpoenas for e-mail content from public ISPs or wireless cellular phone providers. The DoD IG will, however, continue to issue subpoenas for basic subscriber information. *If you need e-mail content for your investigation, you should seek a search warrant. *This is not applicable to DoD or corporate e-mail and telephone communications.

ELECTRONIC DATA		
NO.	**TOPIC**	**COMMENT**
3-7	**Benefits of Requesting Basic Subscriber Information from Internet Service Providers and Telecom Service Providers**	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. Telecom Basic Subscriber Information can provide key information such as all incoming/outgoing calls, to include blocked/restricted calls and also 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.
3-8	**Requests for Reimbursement of Costs Associated with DoD IG Subpoena Compliance**	As with the Right to Financial Privacy Act, the Electronic Communications Privacy Act allows electronic communications providers to be reimbursed for research and copy costs. Forward invoices you receive to the DoD IG Subpoena Program Office for reimbursement.

LEGAL INFORMATION

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-1	**Legal Authority for Issuing a DoD IG Subpoena**	The Inspector General Act of 1978 as amended. 5, U.S.C. § subsection 6(a)(4).
4-2	**Unique Provisions of the Inspector General Act Applicable to the DoD IG**	Section 8 (c) of The Inspector General Act of 1978 as amended, assigns the DoD Inspector General nine unique additional duties, two of which are relevant to the issues of subpoenas. Initiate, conduct, and supervise such audits and investigations in DoD (including military departments) as the IG considers appropriate. Investigate fraud, waste, and abuse uncovered as a result of other contract and internal audits, as the IG considers appropriate.
4-3	**OGC Review of DoD IG Subpoenas**	The DoD IG OGC reviews all requests for DoD IG subpoenas to: ▪ ensure legal enforceability, ▪ ensure admissibility of evidence obtained via subpoena, ▪ help ensure the field agent gets what they need to resolve their investigation, and ▪ prevent inadvertent or intentional overreaching by the IG or Government.

LEGAL INFORMATION

NO.	TOPIC	COMMENT
4-4	**Recipient Refusal to Comply with DoD IG Subpoena (Field Actions)**	If the recipient of the DoD IG subpoena refuses to comply, immediately contact the DoD IG Subpoena Program Office. DoD IG 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 IG OGC. The designated OGC attorney will assist the field agent in preparing an affidavit to be filed in a District Court proceeding. The case agent should be prepared to provide the following information: ▪ detailed information outlining noncompliance, lack of compliance, or partial compliance; copies of subpoena, proof of service, and memorandum requesting subpoena; ▪ copies of all correspondence related to subpoena compliance and/or notes of telephone conversations and e-mail communications; ▪ synopsis detailing efforts to obtain compliance; i.e., telephone calls, discussions, extensions granted; and ▪ synopsis of investigative efforts to date.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-5	**Recipient Refusal to Comply with DoD IG Subpoena (OGC Actions)**	If the recipient of the DoD IG subpoena refuses to comply, immediately contact the DoD IG Subpoena Program Office. DoD IG representatives will get additional information and coordinate with DoJ about enforcement action. The DoD IG OGC will take the following enforcement action steps: ▪ draft decision memorandum to DoJ requesting enforcement, ▪ work with field agent to prepare affidavit concerning facts to date, ▪ may attempt to obtain compliance without DoJ action; shows that Government is trying to be reasonable, and ▪ forward affidavit and case synopsis to DoJ/USAO for action.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-6	**DoD IG OGC Legal Review Criteria for DoD IG Subpoena**	The DoD IG OGC subpoena review criteria are: **Legal Standards** ▪ Is it within the authority of the DoD IG? ▪ Is the demand reasonably relevant to the subject matter of the investigation? ▪ Is the demand overly broad or unduly burdensome? **Additional Factors** ▪ Is the subpoena addressed properly, i.e., custodian of records? ▪ Are company and individual names consistent and spelled correctly? ▪ Is the address correct and consistent? ▪ Is the location of return of service consistent and correct? ▪ Is the DoD nexus clear?
4-7	**Release of Information from a Federal Travel Card Contractor**	12 U.S.C. §3413(q), entitled "Exceptions," Disclosure of information with respect to a Federal contractor-issued travel charge card. 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.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-8	**DoD IG Subpoenas in Support of Non-Fraud Related Investigations**	Subpoenas can be requested for nonfraud-related investigations that satisfy the DoD nexus test criteria. The Defense Criminal Investigation Organization (DCIO) submitting the request must have investigative authority for the crime(s) under investigation and if the investigation is being conducted jointly with another law enforcement organization, the DCIO must be designated as the "lead investigative organization" for that joint investigation. The particular crime at issue must be of such a nature and/or concern to DoD as to warrant the DoD IG's involvement in the investigation. The crimes must be listed in the Particular Crimes matrix that is contained in the DoD IG Memo, "Use of DoD IG Subpoenas in Support of Non-Fraud Related Investigations."
4-9	**Subpoenas for Audits, Projects, and Senior Official Cases**	DoD IG subpoenas issued in support of audit, special projects, senior official investigations, and other DoD IG internal components, must meet the following criteria: ▪ must be a clear DoD nexus, ▪ DoD does not already possess the records, ▪ records are relevant to ascertaining the truth in the matter, ▪ request not unduly broad or burdensome, and ▪ reasonable alternatives have been unsuccessful or are impracticable.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-10	**Subpoenas for Educational Records**	Under the Family Educational Rights and Privacy Act (FERPA), 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. 20 U.S.C. §1232g; 34 CFR Part 99
4-11	**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 DoD IG is able to obtain jurisdiction over the party with records in any necessary enforcement proceeding to obtain the records.
4-12	**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.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-13	**Exceptions to Policy for DoD IG Subpoenas Under the General Crimes Memorandum**	There are occasions when an exception to policy for issuance of a DoD IG subpoena under the General Crimes Memorandum may be appropriate. The case agent should discuss a request for exception to policy with the DoD IG Subpoena Program Office. The DoD IG Subpoena Program Office will discuss the merits and mitigating circumstances for the exception with the OGC attorneys and make a determination. The DoD IG Subpoena Program Office will notify the case agent if an exception to policy will be supported by OGC. Examples of when an exception to the General Crimes Memorandum may be warranted are circumstances or investigations associated with matters when the Subject and/or Victim occupy a senior leadership or a very sensitive and high-visibility position within the DoD and the actions associated with the investigation pose a potential national/international embarrassment to the Department of Defense or Military Service.

LEGAL INFORMATION		
NO.	**TOPIC**	**COMMENT**
4-14	**Service of DoD IG Subpoena After a Qui Tam Case Has Been Filed**	A DoD IG subpoena may be served after a *qui tam* case has been filed because the Government is not a party to a qui tam case until it formally intervenes in the case. (31 U.S.C §3730) Once the DoJ and/or the USAO intervenes in a *qui tam* suit, use of an 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.

OTHER INFORMATION

OTHER INFORMATION		
NO.	**TOPIC**	**COMMENT**
5-1	**Required Case Updates**	Once a DoD IG subpoena is issued, the DoD IG oversees the case. We ask that you keep us informed of the results of subpoena actions and case progress. Place the Subpoena Program Office on distribution for reports of investigation (ROI); and, at a minimum, every ninety (90) days, send updates on the progress of your investigation. Be sure to include the case number and a brief summary of case status, to include actions related to subpoena service. Send updates until the case is closed and all action is taken (report action taken to the Subpoena Program Office as well). You can send your updates via e-mail or hard copy to the DoD IG Subpoena Program Office. When submitting case updates, be sure to include the DoD IG subpoena unique identification number on any correspondence with the DoD IG Subpoena Program Office.

APPENDICES

DOD IG SUBPOENAS IN SUPPORT OF NON FRAUD-RELATED INVESTIGATIONS

DoD IG Subpoenas in Support of Non Fraud-Related Investigations

DOD NEXUS

Is there sufficient DoD nexus to the crime at issue to warrant the DoD IG's involvement in the investigation? Criteria: The Defense Criminal Investigation Organization (DCIO) submitting the request has investigative authority[1] for the crime(s) under investigation and, if the investigation is being conducted jointly with another law enforcement organization, the DCIO has also been designated as the "lead investigative organization" for that joint investigation.[2]

1 For the purpose of this memorandum, the phrase "has investigative authority" means the DCIO has the legal authority to conduct the investigation in question pursuant to its own regulations, and investigative authority has not been specifically reserved to another agency or entity.

2 For example, if a DCIO is supporting local police in an investigation wherein a Service member's car was allegedly stolen from his off-base residence, we would not issue a subpoena for records of the auto dealership where the car was purchased, but would defer to the local police as the "lead" investigative agency.

DoD IG Subpoenas in Support of Non Fraud-Related Investigations

PARTICULAR CRIMES

Is the particular crime at issue of such a nature and/or such concern to DoD as to warrant the DoD IG's involvement in the investigation? Criteria: At least one of the crimes under investigation is an offense listed below.

OFFENSE	U.S.C. CITATION	UCMJ VIOLATION
Murder	18 U.S.C. §1111	UCMJ Article 118
Manslaughter / Death or injury to an unborn child	18 U.S.C. §1112	UCMJ Article 119 UCMJ Article 119a
Attempts to commit murder or manslaughter	18 U.S.C. §1113	UCMJ Article 80
Negligent homicide		UCMJ Article 134 (Homicide, negligent)
Other death investigations conducted by Military Criminal Investigative Organizations (MCIOs)		
Kidnapping	18 U.S.C. §1201 18 U.S.C. §875	UCMJ Article 134 (Kidnapping)
Peonage, slavery, and trafficking in persons	18 U.S.C. Chapter 77	UCMJ Article 133 UCMJ Article 134
Robbery[3]	18 U.S.C. §2111	UCMJ Article 122
Bomb threat or hoax	18 U.S.C. §875	UCMJ Articles 134
Arson or aggravated arson	18 U.S.C. §81	UCMJ Article 126
Unlawful acts involving a firearm	18 U.S.C. Chapter 44	
Maiming	18 U.S.C. §114	UCMJ Article 124
Riot	18 U.S.C. §2101	UCMJ Article 116
Drugs – Unlawful manufacture of, importation of, or trafficking in, a controlled substance [4]	21 U.S.C. §841-843	UCMJ Article 112a

3 Only includes offenses where a firearm (as defined in the Commentary, Applicable Notes 1(e) to §1B1.1 of the Federal Sentencing Guidelines (18 U.S.C. Appendix §1B1.1) was used in the commission of the crime. Restrictions apply to both Title 18 and UCMJ offenses.

4 Only if the quantity of the controlled substance/drug (defined as a substance identified as a controlled substance in §2D1.1 of the Federal Sentencing Guidelines (18 U.S.C. Appendix §2D1.1) involved is, or is reasonably suspected to be, equal to or in excess of the drug quantity specified for Base Offense Level 16 or the Drug Quantity Table found at §2D1.1 of the Federal Sentencing Guidelines (18 U.S.C. Appendix §2D1.1). Restrictions apply to both Title 18 and UCMJ offenses.

DoD IG Subpoenas in Support of Non Fraud-Related Investigations

PARTICULAR CRIMES (Cont'd)

Is the particular crime at issue of such a nature and/or such concern to DoD as to warrant the DoD IG's involvement in the investigation? Criteria: At least one of the crimes under investigation is an offense listed below.

OFFENSE	U.S.C. CITATION	UCMJ VIOLATION
Assault with intent to commit murder, voluntary manslaughter, rape, robbery, sodomy, arson, burglary, or housebreaking	18 U.S.C. Chapter 7	UCMJ Article 120 UCMJ Article 134
Assault in which grievous bodily harm is intentionally inflicted	18 U.S.C. Chapter 7	UCMJ Article 128
Firearm, discharging—willfully, under such circumstances as to endanger human life		UCMJ Article 134
Sexual assault, abuse, or exploitation/Domestic violence and stalking	18 U.S.C. Chapter 109A 18 U.S.C. Chapter 110 18 U.S.C. §2261, §2261A, §2262	UCMJ Article 120 UCMJ Article 120a UCMJ Article 125
Terrorism	18 U.S.C. Chapter 113B	
Espionage	18 U.S.C. §793-798	UCMJ Article 106a
Agent for Foreign Government	18 U.S.C. §951	
Mutiny or sedition and solicitation for same		UCMJ Article 82 UCMJ Article 94
Spies		UCMJ Article 106
Aiding the enemy		UCMJ Article 104
Conspiracy to commit any of the above offenses	18 U.S.C. §371-373	UCMJ Article 81

FORMS REQUIRED FOR ALL DOD IG SUBPOENAS

FORMS		
NO.	**TOPIC**	**COMMENT**
A-1	**Subpoena *Duces Tecum* (Face)**	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. This is the face of the subpoena. It must have the correct legal name of the business or person being subpoenaed. The address for either a person or business must be a physical address (not a Post Office (PO) Box). For businesses, the subpoena should be addressed to the Custodian of Records. The subpoena face will have your physical address for return of service. There will be a return of service date, which is the date the records should be provided. 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 face of the subpoena or can be listed in an Appendix. Even if an Appendix is used, the subpoena face is completed as part of the process to obtain a DoD IG Subpoena. This form is prepared by the DoD IG Subpoena Program Office.
A-2	**Subpoena *Duces Tecum* (Back)**	The back of the subpoena *duces tecum* form contains the Certificate of Return of Service. This is not provided to the subpoena recipient and is completed by the case agent after the subpoena has been served. After the subpoena is served, the case agent completes the Certificate of Return of Service, and scans and e-mails a copy to the DoD IG Subpoena Program Office.

FORMS		
NO.	**TOPIC**	**COMMENT**
A-3	**Appendix**	The Appendix, if needed, is typically completed by the requesting agent to describe the records being subpoenaed. If an Appendix is needed, the DoD IG Subpoena Program Office prefers that requesters e-mail the appendix in Microsoft Word® format in the event the Appendix must be edited or expanded. In most cases, the DoD IG Subpoena Program Office will prepare the final Appendix A, based on a detailed description of records needed that is provided by the requesting agent/investigator.

[FACE OF SUBPOENA FORM]

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 United States Army Criminal Investigation Command (USACIDC) acting on behalf of the Inspector General, pursuant to the Inspector General Act of 1978 (5 U.S.C. App. 3), at USACIDC, Street Address, City or Post, State 00000-0000 on the _____ day of _____, 2009 at 10 o'clock a.m. of that day.

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.

UNIQUE IDENTIFICATION NUMBER:

[BACK OF SUBPOENA FORM]

CERTIFICATE OF RETURN OF SERVICE

I HEREBY CERTIFY that on _____, 2009

at _____, I received the attached subpoena.
(Location)

I further certify that on _____, 2009

at or about _____ m. at _____, I personally
(Time) *(Location)*

served the subpoena upon _____.
(Name and Position or Title)

By _____
(Name)

_____
(Title)

Date _____

UNIQUE IDENTIFICATION NUMBER:

FORMS – REQUIRED FOR ALL SUBPOENAS		
NO.	**TOPIC**	**COMMENT**
A-4	**DoD IG Subpoena Request Memorandum Form**	This form, prepared on agency letterhead, contains 13 interrogatories that provide information about the investigation and documents required. 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.
A-5	**Cover Letter to Subpoena Recipient/Custodian of Records**	The cover letter is completed on agency letterhead by the requesting agent, explains the subpoena requirements, and provides instructions on return of service.

FORMS – REQUIRED FOR ALL SUBPOENAS		
NO.	**TOPIC**	**COMMENT**
A-6	**Privacy Act Notice Form**	The standard Privacy Act Notice is provided for all DoD IG subpoenas.
A-7	**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.

NOTE: PREPARE MEMO ON YOUR AGENCY LETTERHEAD

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

(date)

MEMORANDUM FOR DIRECTOR FOR INVESTIGATIVE POLICY AND OVERSIGHT DEPARTMENT OF DEFENSE

SUBJECT: Request for Inspector General Subpoena

1. Case agent's name:

2. Case agent's office phone number, mobile cellular phone number and fax number:

3. Case agent's electronic email address:

4. Case agent's street address:

5. Case file number:

6. (FOUO-LES) Subject(s) of the investigation**: (Provide complete information on Subject such as rank, title, active duty/reserve status, and Social Security number.)**

7. Date investigation opened:

8. Name of case agent's supervisor who has read this request and approves:

9. Is this a substantive investigation? **(Note: DoD administrative subpoenas are not generally issued for developmental investigations or preliminary inquiries.)**

10. List investigative agencies participating jointly in this investigation, and identify the lead agency.

11. Statute(s) or UCMJ article(s) believed to be violated: **(Provide the full UCMJ or USC Section and title, i.e., UCMJ Article 132, Fraud against the U.S. Government)**

12. (FOUO-LES) Source and reliability of initial information:

13. (FOUO-LES) Summary of information obtained/evidence collected to date suggesting statutes were/are being violated **(It is critical to provide as much detail as possible (who, what, where, when, how, etc.) in order to make a determination as to whether the request meets the criteria for approval:**

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

14. Coordination with prosecutor? Results**?** **(Provide the name of the prosecutor (SJA, AUSA), their concurrence with requesting a subpoena in this matter, whether they believe a crime has been committed, what the crime is, and if they are prepared to prosecute the crime)**

15. Have IG subpoenas been issued previously in this investigation? If so, explain how this (these) subpoena(s) differs. **(Please provide the identity of the subpoena recipient and the DoD IG subpoena number.)**

16. What is the DoD nexus to the records being sought (e.g., they pertain to a DoD contract, a DoD employee of military service member)?

17. What is the time period for the records sought (specific beginning and ending dates)? **How are these dates relevant to your investigation?**

18. 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?

19. What is (are) the proper legal name(s) of the subpoena recipient(s), to include the type of business entity (sole proprietorship, partnership, corporation) if applicable?

20. What is the street address of the subpoena recipient? **(You must list a physical address. Post office boxes cannot be listed)**

21. Why do you believe the subpoena recipient has the records you request?

22. Is the subpoena recipient a bank, credit union, savings and loan, or credit card issuer? If so, what is the full name and Social Security number of the account holder; or, what account number(s) is (are) involved?

23. If the subpoena recipient is not a financial institution, is there another account number or numbers involved? Please list.

24. 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.

25. Have the records sought already been obtained through a search warrant or grand jury subpoena? Has a grand jury been involved? Explain if necessary.

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

26. Do you have any reason to believe this subpoena will be challenged? Explain.

27. How will the records sought assist in this investigation? **Provide specifics as to how the documents are going to support or refute the allegation(s).**

28. Will copies suffice, or do you require original records?

29. Include any other information you believe is important.

30. Individually describe the records, or classes of records you require (subpoena appendix items).

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

(Agency Letterhead)

Custodian of Records

JP Morgan Chase
ATTN: Chase National Subpoena Processing
7610 West Washington St.
Indianapolis, IN 46231

Dear Sir or Madam:

Pursuant to the appendix to subsection 6(a)(4), Title 5, United States Code, the enclosed subpoena *duces tecum* has been issued. The materials identified should be produced by the date and time indicated on the subpoena at:

Air Force Office of Special Investigations
AFOSI Detachment XXXX
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 Air Force Office of Special Investigations (AFOSI) 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 AFOSI 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 to 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 call Special Agent John Public at (000) XXX-XXXX.

Sincerely,

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

Enclosures:

Subpoena Duces Tecum
Appendix A
Privacy Act Notice
Certificate of Compliance

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 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 instances:

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), Section 552, Title 5, U.S.C., 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, Section 552, Title 5, U.S.C., 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

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

_____ _____
(Signature of Respondent) (Date

AGENTS' INSTRUCTIONS CONCERNING SUBPOENAS COVERED BY THE RIGHT TO FINANCIAL PRIVACY ACT

AGENTS' INSTRUCTIONS CONCERNING SUBPOENAS COVERED BY THE RIGHT TO FINANCIAL PRIVACY ACT

The Right to Financial Privacy Act (hereafter, the "Act")[1] 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 memo, cover letter to the subpoena recipient, 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[2]
- Certificate of Compliance[3]

[1] 12 U.S.C. 3401 et seq.

[2] 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.

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).[4] 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 http://www.uscourts.gov/links.html.

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 motion and 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.[5]

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.

[3] 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.

[4] 401 Courthouse Square, Alexandria, VA 22320 (703) 299-2100.

[5] 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.

FORMS REQUIRED FOR ALL SUBPOENAS REQUESTING FINANCIAL RECORDS

FORMS – ALL SUBPOENAS FOR FINANCIAL RECORDS		
NO.	**TOPIC**	**COMMENT**
A-9	**Customer Notice Letter (Subject)**	The customer notice form is completed on agency letterhead and 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 Inspector General of the Department of Defense, c/o DoD IG Subpoena Program Manager, 400 Army Navy Drive, Suite 1037, Arlington, VA 22202.
A-10	**Statement of Customer Rights Form**	The Statement of Customer Rights Form provides a concise explanation of customer rights under the RFPA.
A-11	**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.
A-12	**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.

FORMS – ALL SUBPOENAS FOR FINANCIAL RECORDS		
NO.	**TOPIC**	**COMMENT**
A-13	**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.
A-14	**Certificate of Service Form (Customer Notification to DoD IG)**	This form provides the customer whose records are being subpoenaed, a means of notifying the DoD IG Subpoena Program Manager of a challenge to the subpoena.
A-15	**Agent Certificate of Compliance (Agent Provides to Financial Institution)**	This form is prepared on agency letterhead and certifies to the financial institution that the agent/investigator complied with all of the requirements of the RFPA.

(Agency Letterhead)

CUSTOMER NOTICE

MSgt John Q. Public
1234 Main Street
Anywhere, VA 12345

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 3401-3422, 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, violations 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:

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

Southern District Court of Mississippi
James O. Eastland U.S. Courthouse
245 East Capitol Street, Room 316
Jackson, MS 39201
(601) 965-4439

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

(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, c/o DoD IG Subpoena Program Office, 4800 Mark Center Drive, Suite 11H25, West Tower, 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 10 days from the date of service or 14 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
XXXXXXXXXXXXXXX

Enclosures:

Subpoena Duces Tecum
Appendix
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 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 3 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:
Agency:
Address:
Phone:

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 attachment 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 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 appears on the Customer Notice.

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.	)	MOTION FOR ORDER PURSUANT
)		TO CUSTOMER CHALLENGE
Department of Defense	)	PROVISIONS OF THE RIGHT TO
	)	FINANCIAL PRIVACY ACT
Respondent	)	OF 1978.

_____ hereby move this Court pursuant to
(Your Name)

Section 3410, title 12, United States Code, 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, Section 3410, Title 12, United States Code,

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)
)
) SWORN STATEMENT OF MOVANT
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
(Name of Financial Institution)

being 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, Section 3410, Title 12, United States Code

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

(Agency Letterhead)

(Case Agent's Name)
(Physical Address)
(City, State, Zip Code)

(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, Section 3401, Title 12, United States Code, 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.

(Case agent's signature block)

RESOURCES

Business Identification Number Cross-Reference System (BINCS)

The Business Identification Number Cross-Reference System (BINCS) is a search engine of manufacturers and suppliers. Information on this system is cross-referenced to permit inquiry by CAGE, DUNS, company name, phone number, SIC Code, and zip code.

Website Address: https://www.bpn.gov/bincs/

U.S. District Court Links

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

Website Address: http://www.uscourts.gov/courtlinks/

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: http://www.search.org/programs/hightech/isp/

4. Central Contractor Registration

Central Contractor Registration (CCR) is the primary registrant database for the U.S. Federal Government. CCR collects, validates, stores, and disseminates data in support of agency acquisition missions, including Federal agency contract and assistance awards.

Website Address: https://www.bpn.gov/CCRSearch/Search.aspx

Fraud Investigator's Toolkit

Several links helpful in the investigation of fraud matters can be found in the "Fraud Investigator's Toolkit" on the DoD IG, Investigative Policy and Oversight, website.

Website Address: http://www.dodig.mil/Inspections/

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/

ADMINISTRATIVE REMINDERS

ADMINISTRATIVE REMINDERS

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

Include the cellular phone number of case agent.

When providing addresses, do not use post office boxes, a physical address must be listed.

Zip codes must match the physical address.

If the investigation is being conducted jointly with other law enforcement agencies, identify the lead investigative agency.

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

Be sure to include the Subject's full information such as rank, active duty status (Active, Guard, Reserve) and last four digits of their Social Security number. [Section 6]

When listing the statutes, provide the full 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. [Section 11]

When providing the Summary of Investigation, provide sufficient details for the DoD IG Subpoena Program Office and the Office of General Counsel to make a determination of whether the subpoena request is justified. [Section 13]

If previous DoD IG subpoenas have been issued, identify the subpoena recipient and the DoD IG subpoena Unique Identification Number. If this request is for the same recipient, explain how these requested records differ from those previously obtained/requested.

Provide the name of the prosecutor (SJA, AUSA), their concurrence with requesting a subpoena in this matter, whether they believe a crime has been committed, what the crime is, and if they are prepared to prosecute the crime. [Section 14]

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. [Sections 17 and 27]

When sending request package and forms, if you are sending the documents in pdf. format, please also include identical documents in Microsoft Word version.

Make sure that all interrogatories on the DoD IG Subpoena Request Memo are numbered correctly.

SUBPOENA REQUEST CHECKLIST

DOD INSPECTOR GENERAL SUBPOENA REQUEST CHECKLIST

STANDARD SUBPOENA REQUEST

√	FORM	REFERENCE
	Inspector General Subpoena Request Memo	A-4, Pages 51-53
	Subpoena Cover Letter (Memo to Custodian of Records/Subpoena Recipient)	A-5, Pages 54-55
	Notice Pursuant to Privacy Act of 1974	A-6, Pages 56-57
	Certificate of Compliance (completed by Custodian of Records/Subpoena Recipient)	A-7, Page 58
	Appendix (if required)	A-3, Pages 90-113

FINANCIAL RECORDS SUBPOENA REQUEST

√	FORM	REFERENCE
	Standard Subpoena Request Documents (see above)	Pages 51-58; Page 113
	Customer Notice Letter	A-9, Pages 66-67
	Statement of Customer Rights under the Right to Financial Privacy Act (RFPA)	A-10, Page 68
	Instructions for Completing and Filing a Motion and Sworn Statement	A-11, Page 69
	Blank Motion Form	A-12, Page 70
	Blank Statement Form	A-13, Page 71
	Certificate of Service (completed by Customer and forwarded to DoD IG Subpoena Program Office)	A-14, Page 72
	Certificate of Compliance with RFPA (completed by Special Agent and provided to financial institution that is receiving the subpoena)	A-15, Page 73

ELECTRONIC RECORDS SUBPOENA REQUEST

√	FORM	REFERENCE
	Standard Subpoena Request Documents (see above)	Pages 51-58; Pages 109-113

DOD INSPECTOR GENERAL SUBPOENA REQUEST CHECKLIST

ADMINISTRATIVE

√	TOPIC	REFERENCE
	After service of subpoena, complete Certificate of Return of Service (back of subpoena), scan it, and forward to DoD IG Subpoena Program Office.	Section 1-5, Page 9; A-2, Page 48
	Ensure copy of case updates are provided to DoD IG Subpoena Program Office every 90 days.	Section 5-1, Page 38
	If you encounter any problems with the service of the subpoena or determine that a challenge has been filed under the RFPA, immediately notify the DoD IG Subpoena Program Office.	Section 1-6, Page 10; Section 2-12, Page 21; Section 4-4, Page 30
	If you receive an invoice from a financial institution or electronic communications provider requesting reimbursement of costs for providing documents, contact the DoD IG Subpoena Program Office.	Section 2-11, Page 20; Section 3-8, Page 27

INVESTIGATIVE PLANNING CONSIDERATIONS

INVESTIGATIVE PLANNING CONSIDERATIONS

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.

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.

SAMPLE SUBPOENA REQUEST MEMO

(Agency Letterhead)

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

MEMORANDUM FOR DIRECTOR FOR INVESTIGATIVE POLICY AND OVERSIGHT DEPARTMENT OF DEFENSE

SUBJECT: Request for Inspector General Subpoena

1. Case agent's name: **Special Agent John Smith**

2. Case agent's office phone number, mobile cellular phone number and fax number: **(703) 604-8700; (703) 604-8720; (703) 604-8701**

3. Case agent's electronic email address: **john.smith@usmil.com**

4. Case agent's street address: **Maryland Fraud Resident Agency, Major Procurement Fraud Unit, US Army Criminal Investigation Division, 5115 Pistol Road, Aberdeen Proving Ground, MD 21005**

5. Case file number: **0000-2006-CID000-000**

6. (FOUO-LES) Subject(s) of the investigation: (Provide complete information on Subject such as rank, title, active duty/reserve status, and Social Security number): **ACME International, Inc., 1234 Box Hill Corporate Center, Suite B, Somewhere, MD 21001-1234**

7. Date investigation opened: **May 21, 2004**

8. Name of case agent's supervisor who has read this request and approves: **John Doe, Resident Agent in Charge, (410) 832-4510**

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

10. List investigative agencies participating jointly in this investigation. **None.**

11. Statute(s) or UCMJ article(s) believed to be violated: (Provide the full UCMJ or USC Section and title, i.e., UCMJ Article, Fraud against the U.S. Government) **18 U.S.C. §287, False Claims and 18 U.S.C. §1001, False Statements**

Does the violation/crime fall within the Statute of Limitations? **Yes**

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

12. (FOUO-LES) Source and reliability of initial information: **Dr. Joe Stevens, President of Tri Tech Services Inc., 1234 Woodbridge Way, Edgewood, MD 22232, a sub contractor to ACME International, Inc., on contract DAAD00-03-D-11221. Dr. Stevens is considered reliable due to his unique knowledge of the contract (he was the prime on the previous contract for the same services) and his knowledge of the employee's qualifications (many of ACME's employees were previously employed by Tri Tech.**

13. (FOUO-LES) Summary of information obtained/evidence collected to date suggesting statutes were/are being violated (Include sufficient detail to understand the who, what, where, when, how, etc.): **This investigation was initiated based on information received from Dr. Joe Stevens, President, Tri Tech Services, Inc., (Tri Tech), 1234 Woodbridge Way, Edgewood, MD 22232.**

On 15 Jun 03, the U.S. Army Solder and Biological Chemical Command (SBCCOM), now the research development and engineering command (RDECOM), awarded ACME International, Inc. (ACME) an indefinite quantity/indefinite delivery contract with time and materials task orders for environmental sciences support, contract number DAAD00-03-D-11221, with a five year performance period, valued at $20,000,000.00. ACME subsequently subcontracted a portion of the work to Tri Tech.

Dr. Stevens alleged ACME 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.

14. Coordination with prosecutor? Results? (Provide the name of the prosecutor (SJA, AUSA), their concurrence with requesting a subpoena in this matter, whether they believe a crime has been committed, what the crime is, and if they are prepared to prosecute the crime) **This investigation was coordinated with AUSA Bob Smith, AUSA Office, Baltimore, MD, who concurred with the request for a DoD IG subpoena to obtain the necessary records and documents.**

15. Have IG subpoenas been issued previously in this investigation? If so, please explain. (Please provide the identity of the subpoena recipient and the DoD IG subpoena number) **No subpoenas have been previously issued.**

16. What is the DoD nexus to the records being sought (e.g., they pertain to a DoD contract, a DoD employee of military service member**)? The records being sought are related to ACME's contract, DAAD00-03-D-11221, with the U.S. Army.**

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

17. What is the time period for the records sought (specific beginning and ending dates)? How are these dates relevant to your investigation**? From 15 Jun 2003 to present, ACME has submitted numerous invoices to the government and has been paid about $2.4 million for those invoices. It is believed those invoices included fraudulent billings for labor costs.**

18. 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. Patricia Jones, Contracting Officer, Robert Ames Acquisition Center – Edgewood Branch, APG, MD 22232; 15 Jun 2003 through 14 Jun 2008; Environmental Services Support.**

19. What is (are) the proper legal name(s) of the subpoena recipient(s), to include the type of business entity (sole proprietorship, partnership, corporation) if applicable? **ACME International, Incorporated.**

20. What is the street address of the subpoena recipient? (you must list a physical address. Post office boxes cannot be listed) **1234 Box Hill Corporate Center, Suite B, Somewhere, MD 21001-1234.**

21. Why do you believe the subpoena recipient has the records you request? **These records are required by the contract to be maintained by the contractor. These are normal business records that would be maintained by any normal business.**

22. Is the subpoena recipient a bank, credit union, savings and loan, or credit card issuer? If so, what is the full name and Social Security number of the account holder; or, what account number(s) is (are) involved? **Not Applicable.**

23. If the subpoena recipient is not a financial institution, is there another account number or numbers involved? Please list. **Not Applicable.**

24. 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. **These records are not believed to be in the possession of any other federal agency.**

25. Have the records sought already been obtained through a search warrant or grand jury subpoena? Has a grand jury been involved? Explain if necessary. **No.**

26. Do you have any reason to believe this subpoena will be challenged? Explain. **No.**

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

FOR OFFICIAL USE ONLY Law Enforcement Sensitive

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

28. Will copies suffice, or do you require original records? **Certified copies will suffice.**

29. Include any other information you believe is important.

30. Individually describe the records, or classes of records you require (subpoena appendix items). **Certified payroll documents pertaining to all invoices submitted under contract DAAD00-03-D-11221; complete resumes for all employees who have had hours billed to contract DAAD00-03-D-11221; all documents used to substantiate labor hours and labor categories on invoices submitted under contract DAAD00-03-D-11221.**

SAMPLE APPENDIX A

PROCUREMENT FRAUD INVESTIGATIONS

APPENDIX A
(Insert Company's Name)

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 nonidentical 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 nonidentical copy.

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

4. "XXXX" means the Defense Criminal Investigative Organization.

5. "Company Name" means *(*Company's Full Name) Group, Inc. and any parents, 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.

6. "Secondary Company Name" means "Company's Full Name" and any parents, 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. "You" or "your" means the person or entity listed as the recipient of this subpoena. If an entity, "you" or "your" includes any 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.

8. The term "Contract(s)" or "Contracts at Issue" means contract number(s) M00264-08-D-001 between (Company Name) and the USMC, through prime contractor JWT, and all modifications or extensions to the contract.

9. 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.

10. 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.

11. 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."

12. 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.

13. "Concerning" means referring to, describing, evidencing, or constituting.

14. "Communication" means the transmittal of information (in the form of facts, ideas, inquiries, or otherwise).

15. 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.

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 *Recipient*. Questions concerning the compatibility of the software should be addressed with Special Agent _____ at _____ (phone number).

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 (for example, 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. 1. 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, that 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; for example., "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 DCIS 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 noncompliance with the subpoena.

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.

DOCUMENTS REQUIRED

1. Any and all documents relating to contracts between *(*Company Name) Group, Inc. and the Department of Defense and/or prime contractors, including but not limited to contract M00XXX-08-D-0001, for the period of December 1, 2007, to the date of this subpoena, including, but not limited to:

2. 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.

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

4. 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.

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

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

7. Any and all inventory files and analyses.

8. 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.

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

10. 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: the 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.

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

12. Any and all documentation pertaining to inspections of work performed by (Company Name) for Department of Defense contract number M00264-08-D-0001.

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

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

15. Any and all documents pertaining to negotiations between ACME and the Department of Defense and/or prime contractors.

16. 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.

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

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

19. All subcontract agreements with applicable support relevant to the Department of Defense contract between December 1, 2007, to the date of this subpoena.

20. Any and all lists of any and all customers both commercial and Government, with whom (Company Name) was working from December 1, 2007, through the date of this subpoena. Any and all lists of jobs, both commercial and Government, that ACME was working on from December 1, 2007, to the date of this subpoena.

21. Any and all lists of all (Company Name) employees who have worked on Department of Defense contracts from December 1, 2007, to the date of this subpoena.

SAMPLE APPENDIX B
(DIGITAL MEDIA SPECIFICATIONS)

PROCUREMENT FRAUD INVESTIGATIONS

APPENDIX B

Specifications for Production of Electronically Stored Information and Digitized ("Scanned") Images ("Production Specifications")

To the extent possible, electronically stored information and digitized (scanned) images should be produced in accordance with the specifications below:

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.

1. Specification Modifications
Any modifications or deviations from the production specifications may be done only with the express permission of the Department of Defense, Office of Inspector General ("DoD OIG"). Any responsive data or documents that exist in locations or native forms not discussed in these production specifications remain responsive; therefore, arrangements should be made with the DoD OIG to facilitate their production.

2. Production Format of ESI and Imaged Hard Copy
Responsive ESI and imaged hard copy shall be produced in the format outlined below. All ESI, except as outlined in sections 9 through 18, shall be rendered to type TIFF image format and accompanied by a Concordance Image Cross-Reference file. All applicable metadata (see section 3) shall be extracted and provided in Concordance load file format.

a. Image File Format: All images, paper documents scanned to images, or rendered ESI, shall be produced as 300 dpi single-page TIFF files, CCITT Group IV (2D Compression). Documents should be uniquely and sequentially Bates numbered with an endorsement burned into each image.

- ☐ All TIFF file names shall include the unique Bates number burned into the image.
- ☐ Each Bates number shall be a standard length, include leading zeros in the number, and be unique for each produced page.
- ☐ All TIFF image files shall be stored with the ".tif" extension.
- ☐ Images should be able to be OCR'd using standard COTS products, such as LexisNexis LAW PreDiscovery.
- ☐ All pages of a document or all pages of a collection of documents that comprise a folder or other logical grouping, including a box, should be delivered on a single piece of media.
- ☐ No image folder shall contain more than 2,000 images.

b. Concordance Image Cross-Reference File: Images should be accompanied by a Concordance Image Cross-Reference file that associates each Bates number with its corresponding single-page TIFF image file. The Cross-Reference file should also contain the image file path for each Bates numbered page.

☐Image Cross-Reference Sample Format:

ABC00000001,OLS,D:\DatabaseName\Images\001\ ABC00000001.TIF,Y,,,
ABC00000002,OLS,D:\DatabaseName\Images\001\ ABC00000002.TIF,,,,
ABC00000003,OLS,D:\DatabaseName\Images\001\ ABC00000003.TIF,,,,
ABC00000004,OLS,D:\DatabaseName\Images\001\ ABC00000004.TIF,Y,,,

c. Concordance Load File: Images should also be accompanied by a "text load file" containing delimited text that will populate fields in a searchable, flat database environment. The file should contain the required fields listed in section 3.

☐ASCII text delimited load files are defined using the following delimiters:

Field Separator ^ *or Code 094*
Text Qualifier | *or Code 124*
Substitute Carriage Return or New Line () or Code 013

- The text file should also contain hyperlinks to applicable native files, such as Microsoft Excel or PowerPoint files.
- There should be one line for every record in a collection.
- The load file must contain a field map/key listing the metadata/database fields in the order they appear within the data file. For example, if the data file consists of a First Page of a Record (starting Bates), Last Page of a Record (ending Bates), Document ID, Document Date, File Name, and a Title, then the structure may appear as follows:

|BEGDOC#|^|ENDDOC#|^|DOCID|^|DOCDATE|^|FILENAME|^|TITLE|

- The extracted/OCR text for each document should be provided 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.

3. Required Metadata/Database Fields

- A "✓" denotes that the indicated field should be present in the load file produced.
- "Other ESI" includes e-mail or hard copy documents, including but not limited to data discussed in sections 6 through 9 and 12 through 18.

Field Name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
COMPANY	Company/organization submitting data	Full Text	Unlimited	✓	✓	✓
BOX#	Submission/volume/box number	Note Text	10	✓	✓	✓
CUSTODIAN	Custodian(s)/source(s) - format: last, first or ABC dept.	Multi-entry	Unlimited	✓	✓	✓
AUTHOR	Creator of the document	Note Text	160			✓
BEGDOC#	Start Bates (including prefix) - no spaces	Note Text	60	✓	✓	✓
ENDDOC#	End Bates (including prefix) - no spaces	Note Text	60	✓	✓	✓
DOCID	Unique document Bates # or populate with the same value as Start Bates (DOCID = BEGDOC#)	Note Text	60	✓	✓	✓
PGCOUNT	Page count	Integer	10	✓	✓	✓
PARENTID	Parent's DOCID or parent's start Bates (for EVERY document including all child documents)	Note Text	60	✓	✓	✓
ATTACHIDs	Child document list; child DOCID or child start Bates	Multi-entry	60	✓	✓	✓
ATTACHLIST	List of attachment Bates numbers	Multi-entry	Unlimited		✓	✓
BEGATTACH	Start Bates number of first attachment	Note Text	60	✓	✓	✓
ENDATTACH	End Bates number of last attachment	Note Text	60	✓	✓	✓

Field Name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
PROPERTIES	Privilege notations, redacted, document withheld based on privilege	Multi-entry	Unlimited	✓	✓	✓
RECORD TYPE	File, e-mail, attachment, or hardcopy	Note Text	60	✓	✓	✓
FROM	Author - format: last name, first name	Note Text	160		✓	✓
TO	Recipient- format: last name, first name	Multi-entry	Unlimited		✓	✓
CC	Carbon copy recipients - format: last name, first name	Multi-entry	Unlimited		✓	✓
BCC	Blind carbon copy recipients - format: last name, first name	Multi-entry	Unlimited		✓	✓
SUBJECT	Subject/document title	Note Text	Unlimited		✓	✓
DOCDATE	Document date/date sent - format MM/DD/YYYYY	Date Keyed	MM/DD/YYYY			✓
BODY	E-mail body, other electronic document extracted text, or OCR	Full Text	Unlimited	✓	✓	✓
TIMESENT	Time e-mail was sent	Time	10		✓	
DATECRTD	Date created	Date	MM/DD/YYYY		✓	✓
DATESVD	Date saved	Date	MM/DD/YYYY		✓	✓
DATEMOD	Date last modified	Date Keyed	MM/DD/YYYY		✓	✓
DATERCVD	Date received	Date	MM/DD/YYYY		✓	
DATEACCD	Date accessed	Date	MM/DD/YYYY		✓	✓
FILESIZE	File size	Note Text	10			✓
FILENAME	File name - name of file as it appeared in its original location	Full Text	Unlimited			✓
APPLICATION	Application used to create native file (e.g. Excel, Outlook, Word)	Note Text	160		✓	✓
FILEPATH	Original data source full folder path	Full Text	Unlimited		✓	✓
NATIVELINK	Current file path location to the native file	Full Text	Unlimited		✓	✓
FOLDERID	E-mail folder path (e.g., inbox\active) or hard copy container information (e.g., folder or binder name)	Full Text	Unlimited	✓	✓	
PARAGRAPH	Subpoena/request paragraph number to which the document is responsive	Multi-entry	Unlimited	✓	✓	✓

Field Name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
HASH	Hash value (used for deduplication or other processing) (e-mail hash values must be run with the e-mail and all of its	Note Text	Unlimited		✓	✓
MESSAGEHEADER	E-mail header. Can contain IP address	Full Text	Unlimited		✓	
ATTACHMCOUNT	Number of attachments to an e-mail	Note Text	10		✓	
FILETYPE	Identifies the application that created the file	Note Text	160		✓	✓
COMMENTS	Identifies whether the document has comments	Note Text	10		✓	✓

4. De-duplication, Near-Duplicate Identification, E-mail Conversation Threading, and Other Culling Procedures

De-duplication of exact copies *within* a custodian's data may be done, but all "filepaths" must be provided for each duplicate document. The recipient shall not use any other procedure to cull, filter, group, separate, or de-duplicate (i.e., reduce the volume of) responsive material before discussing with and obtaining the written approval of the DoD OIG. All objective coding (e.g., near dupe ID or e-mail thread ID) shall be discussed and produced for the DoD OIG as additional metadata fields.

5. Hidden Text

All hidden text (e.g., track changes, hidden columns, mark-ups, notes) shall be expanded and rendered in the image file. For files that cannot be expanded, the native files shall be produced with the image file.

6. Embedded Files

All nongraphic 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.

7. Image-Only Files

All image-only files (nonsearchable .pdfs, multipage TIFFs, Snipping Tool [and other] screenshots, etc., as well as all other images that contain text) shall be produced with the associated OCR text and metadata/database fields identified in the "Other ESI" column in the table in section 3.

8. Hard Copy Records

a. All hard copy material shall reflect accurate document unitization including all attachments and container information (to be reflected in the ParentID, AttachID, beg attach, end attach and group ID). 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). The first document in the collection represents the parent document and all other documents will represent the children.

b. 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.

c. All objective coding (e.g., document date or document author) should be discussed and produced for the DoD OIG as additional metadata/database fields.

9. 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). See section 18 below. The file produced should maintain the integrity of all source, custodian, application, embedded, and related file system metadata. No alteration shall be made to file names or extensions for responsive native electronic files.

10. 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, and tasks. For purposes of production, responsive items shall include the "E-mail" metadata/database fields outlined in section 3, including but not limited to all parent items (mail, calendar, contacts, tasks, notes, etc.) and child files (attachments of files to e-mail or other items) with the parent/child relationship preserved. E-mail databases from operating systems other than Microsoft Exchange shall be produced after consultation with and written consent of the DoD OIG about the format for the production of such databases.

11. Production of Items Originally Generated in E-Mail Repositories but Found and Collected Outside of E-mail Repositories, For Example, 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 like .MSG, .HTM, .MHT, etc.), shall be produced with the "E-mail" metadata fields outlined in section 3, including but not limited to any attachments, maintaining the family (parent/child) relationship.

12. Production of Instant Messenger (IM), Voicemail Data, Audio Data, and Video Data

The responding party shall identify, collect, and produce any and all data that are responsive to the requests. The data may be stored in audio or video recordings, cell phone/PDA/Blackberry/smart phone data, voicemail messaging data, instant messaging, text messaging, conference call data, and related/similar technologies. However, such data, logs, metadata, or other files related thereto, as well as other less common but similar data types, shall be produced after consultation with and written consent of the DoD OIG about the format for the production of such data.

13. Productions of Structured Data
Prior to any production of responsive data from a structured database (e.g., Oracle, SAP, SQL, MySQL, QuickBooks, etc.), the producing party shall first provide the database dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be provided in native Excel (.xls) format.

14. Productions of Structured Data from Proprietary Applications
Prior to any production of structured data from proprietary applications (e.g., proprietary timekeeping, accounting, sales rep call notes, etc.) the producing party shall first provide the database dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be produced in native Excel (.xls) format.

15. Production of Photographs with Native File or Digitized ESI
Photographs shall be produced as single-page .JPG files with a resolution equivalent to the original image as it was captured/created. All .JPG files shall have extracted metadata/database fields provided in a Concordance load file format as identified in the "Other ESI" column in the table in section 3.

16. OCR Text Conversion Exception
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 electronic Bates, document, id or Bates number(s) corresponding to each such image.

17. Format of ESI from Non-PC or Windows-Based Systems
If responsive ESI is in non-PC or non-Windows-based Systems (e.g., Apple, IBM mainframes and UNIX machines), the ESI shall be produced after discussion with and written consent of the DoD OIG about the format for the production of such data.

18. Production of Native Files (When Applicable Pursuant to These Specifications)
Productions 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 identified in the "Other ESI" column in the table in section 3.

ESI shall be produced in a manner that is functionally useable by the DoD OIG. The following are examples:

- AutoCAD data, (e.g., .DWG, .DXF) shall be processed/converted and produced as single-page . JPG image files and accompanied by a Concordance Image formatted load 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.

- 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.

- 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).

19. Bates Number Convention

All images should be assigned Bates numbers before production to DoD OIG. The numbers should be "endorsed" (or "burned in") on the actual images. Native files should be assigned a single bates number for the entire file. 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 name/number common to each page (when assigned to an image) or to each document (when assigned to a native file). If DoD OIG agrees to a rolling production, the naming/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:

PREFIX0000001	PREFIX0000003
PREFIX0000001.001	PREFIX0000003.001
PREFIX0000001.002	PREFIX0000003.002

20. 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.

b. External hard drives, USB 2.0 (or better) or eSATA, formatted to NTFS format specifications. c. Storage media used to deliver ESI shall be appropriate to the size of the data in the production. d. Media should be labeled with the case name, production date, Bates range, and producing party.

21. 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 DoD OIG. Password protected or encrypted files or media shall be provided with corresponding passwords and specific decryption instructions. No encryption software shall be used without the written consent of DoD OIG.

22. 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), U.S. National Archives & Records Administration ("NARA" at www.archives.gov), American Records Management Association ("ARMA International" at www.arma.org), American National Standards Institute ("ANSI" at www.ansi.org), International Organization for Standardization ("ISO" at www.iso.org), and/or other U.S. Government or professional organizations.

23. 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.

24. Exception Log
An Exception Log shall be included documenting any production anomalies utilizing by the electronic Bates number (document id or control numbering) assigned during the collection, processing and production phases.

25. Privilege Logs
Productions that include claims of privilege or confidentiality, (resulting in documents, or portions of documents, being withheld), shall be accompanied by a Privilege Log that identifies the document(s) by Bates range and the basis for each claim or privilege. The Privilege Log shall be electronically produced in native Excel (.xls) or Access (.mdb) and for any document withheld on the ground of any claimed privilege shall include:

a. The name and title of the author (and if different, the preparer and signatory);

b. The name(s) and title(s) of the individual(s) to whom the document was addressed;

c. The name(s) and title(s) of the individuals to whom the document or a copy of the document was sent or to whom the document or a copy, or any part thereof, was shown;

d. The date of the document;

e. The number of pages;

f. A brief description of the subject matter;

g. A statement of the specific basis on which privilege is claimed; and

h. The subpoena request to which it is responsive.

26. Transmittal Letter to Accompany Deliverables
All deliverables shall be accompanied by a transmittal letter including all of the following information at a minimum: production date, subpoena request responding to, identity of producing party, production volume name, electronic Bates number (document id or control numbering), and Bates number ranges referenced, custodian names, and total number of records.

SAMPLE APPENDIX A

INTERNET SERVICE PROVIDER (ISP)

APPENDIX A

A. INSTRUCTIONS

This subpoena calls for the production of records setting forth the basic subscriber information identified below, authorized by the Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.), pertaining to the [*insert name of Internet Service Provider , i.e., Yahoo! Incorporated*] email address/Internet Protocol (IP) address "[*insert screen name, Internet Protocol Address, etc.*]" believed to be utilized by and/or associated with *[enter name of Subject; the unauthorized access to a Department of Defense computer system*], for the period January X, 2009, through the date of this subpoena.

B. REQUIRED RECORDS

1. All names associated with the account(s);

2. All addresses associated with the account(s);

3. Local and long distance telephone connection records and/or records of session times and durations, including connection dates and times, disconnect dates and times, and methods of connection;

4. Length of service, including start date, end date (if applicable), and types of services used;

5. Telephone or instrument number(s) and/or other subscriber number(s) or identities, including any temporarily assigned network address; and,

6. Means and source of payment for service (including any credit card or bank account number).

SAMPLE APPENDIX A

MOBILE CELLULAR PHONE CARRIER

APPENDIX A

REQUIRED RECORDS:

This subpoena requires the production of records setting forth the basic subscriber information below concerning [*insert mobile cellular phone company name*] cellular phone services pertaining to phone numbers [*insert phone number to include area code*], believed to utilized by and/or associated with [*insert name*], an active duty member, of the United States [*insert branch of service*], who is suspected of violating one or more punitive Articles of the Uniform Code of Military Justice, for the period January X, 2010, through the date of this subpoena.

1. All names associated with the account(s);

2. All addresses associated with the account(s);

3. Local and long distance telephone connection records (to include telephone call detail and alpha numeric 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. Length of service, including start date, end date (if applicable), and types of services used;

5. Telephone or instrument number(s) and/or other subscriber number(s) or identities, including any temporarily assigned network address; and,

6. Means and source of payment for service (including any credit card or bank account number).

SAMPLE APPENDIX A
FINANCIAL RECORDS

APPENDIX A

A. DEFINITIONS:

1. The terms “document” or “documents” mean any written, recorded, graphic material of any kind, 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” mean 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.

B. REQUIRED RECORDS:

Any and all records pertaining to XXXXX Federal Savings Bank account number XXXXXXXX, held solely or jointly by XXXXXXXXXXX, Social Security number: XXX-XX-XXXX, a member of the United States Air Force Reserve, who is suspected of committing one or more punitive Articles of the Uniform Code of Military Justice, for the period January 1, 2004, through the date of this subpoena. Records include, but are not limited to:

1. Monthly statements sent to the account holder;
2. Correspondence with the account holder;
3. Deposit records;
4. Withdrawal records;
5. Wire transfer records;
6. Records of Automatic Teller Machine transactions;
7. Records of debit and credit card transactions;
8. Copies of checks written on the named account and/or deposited into the named account; and,
9. Records reflecting account ownership in effect during the identified period.
10. Loan(s) and loan application(s).

EXAMPLE OF MEMO GRANTING REQUEST FOR EXTENSION ON SUBPOENA COMPLIANCE DATE

Agency Letterhead

FROM: Special Agent XXXXXXX

TO: Mr. XXXXX
Legal Representative for XXXX Corporation
XXXXXXXXXXXXXXXXXXXX

SUBJECT: Request for Subpoena Compliance – XXXXX Corporation

On September 10, 2010, Special Agent XXXXXX spoke with Mr. XXXXXXX, Legal Representative for XXX Corporation, XXXXXXXXXXXXXX, Washington, D.C. Mr. XXXXXX, as XXXXX Corporation's Legal Representative, has requested a sixty (60) day extension to the original subpoena compliance date of September XX, 20XX, for DoD IG Subpoena Unique Identification Number: 2010XXX-XXXXX, which was served on August XX, 20XX.

This Memorandum serves as an understanding between Mr. XXXXX and XXXXX, that a good faith effort will be made by XXXX Corporation to produce requested documents, initially on a prioritization basis based on concurrence with Special Agent XXXXXXXX. The production of records will be on a rolling basis and will commence no later than October 15, 2010. 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 AFOSI XXXXX. If there are any questions or concerns, please contact Special Agent XXXXXX at XXXXXXX or via email at XXXXXXX. Request that you sign and date this memo below and return to Special Agent XXXXXX at facsimile number XXXXX.

XXXXXXXX, Special Agent
XXXXXXXXXXXXX

ACKNOWLEDGEMENT:

As an agent of XXXX Corporation, I hereby acknowledge that XXXX 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)

CRIMINAL AND CIVIL STATUTES WITH POTENTIAL APPLICATION TO FRAUD INVESTIGATIONS

CRIMINAL AND CIVIL STATUTES WITH POTENTIAL APPLICATION TO FRAUD INVESTIGATIONS

STATUTE	TITLE
10 U.S.C. §2306a	Truth in Negotiations Act (TINA)
10 U.S.C. §2408	Prohibition on Persons Convicted of Defense Contract Related Felonies
15 U.S.C. §1	Sherman Anti-Trust Act
15 U.S.C. §1124	Importation of Goods Bearing Infringing Marks or Names Forbidden
15 U.S.C. §1125	False Description [geographic] Origin, False Description, and Dilution Forbidden
15 U.S.C. §5408	Remedies and Penalties Under the Fastener Quality Act of 1990, as Amended
18 U.S.C. §38	Fraud Involving Aircraft or Space Vehicle Parts in Interstate or Foreign Commerce
18 U.S.C. §201	Bribery
18 U.S.C. §203	Outside Compensation
18 U.S.C. §205	Activities of Officers and Employees in Claims Against the U.S. Government
18 U.S.C. §207	Restrictions on Former Officers and Employees
18 U.S.C. §208	Acts Affecting a Personal Financial Interest
18 U.S.C. §286	Conspiracy to Defraud the U.S. Government
18 U.S.C. §287	False Claims
18 U.S.C. §371	Conspiracy
18 U.S.C. §641	Theft
18 U.S.C. §666	Theft or Bribery Concerning Programs Receiving Federal funds
18 U.S.C. §1001	False Statements
18 U.S.C. §1030	Fraud and Related Activity in Connection With Computers
18 U.S.C. §1031	Major Fraud
18 U.S.C. §1341	Mail Fraud
18 U.S. C §1343	Wire Fraud
18 U.S.C. §1346	Honest Services
18 U.S.C. §1505	Obstruction of Proceedings Before Departments and Agencies
18 U.S.C. §1510	Obstruction of Criminal Investigations
18 U.S. C §1511	Obstruction of State or Local Law Enforcement
18 U.S.C. §1516	Obstruction of a Federal Audit
18 U.S.C. §1832	Theft of Trade Secrets
18 U.S. C §1905	Trade Secrets Act
18 U.S.C. §2153	Destruction of War Material
18 U.S.C. §2154	Production of Defective War Material
18 U.S. C §2155	Destruction of Material – Defense Material

CRIMINAL AND CIVIL STATUTES WITH POTENTIAL APPLICATION TO FRAUD INVESTIGATIONS

STATUTE	TITLE
19 U.S.C. §2511, *et seq.*	Trade Agreements Act of 1979, as Amended
28 U.S.C. §2514	Forfeiture of Fraudulent Claims Against the United States
31 U.S.C. §3729-§3732	False Claims Act
31 U.S.C. §3801, *et seq.*	Program Fraud Civil Remedies Act of 1986 (PFCRA)
41 U.S.C. §10a - §10d	Buy America Act
41 U.S.C. §15	Anti-Assignment Statute
41 U.S.C. §51, *et seq.*	Anti-Kickback Act
41 U.S.C. §§ 2101	Procurement Integrity Act
41 U.S.C. §604	Fraudulent Claims Under the Contract Disputes Act of 1978

UNIFORM CODE OF MILITARY JUSTICE (UCMJ) ARTICLES WITH POTENTIAL APPLICATION TO FRAUD INVESTIGATIONS

UNIFORM CODE OF MILITARY JUSTICE (UCMJ) ARTICLES WITH POTENTIAL APPLICATION TO FRAUD INVESTIGATIONS

ARTICLE	TITLE
UCMJ Article 81	Conspiracy
UCMJ Article 83	Fraudulent Enlistment, Appointment, or Separation
UCMJ Article 84	Effecting Unlawful Enlistment, Appoint or Separation
UCMJ Article 107	False Official Statement
UCMJ Article 108	Military Property of the United States – Sale, Loss, Damage or Destruction or Wrongful Disposition
UCMJ Article 121	Larceny and Wrongful Appropriation
UCMJ Article 123	Forgery
UCMJ Article 123(a)	Making, Drawing, or Uttering Check, Draft, or Order Without Sufficient Funds
UCMJ Article 132	Frauds Against the United States
UCMJ Article 134	Bribery and Graft
UCMJ Article 134	Obtaining Services Under False Pretenses