Who We Are

• We are an independent oversight function overseeing DOC operations, and are primarily staffed with:
  – Special Agents / Investigators / Attorneys
  – Auditors and Evaluators

• Our responsibility is to pursue allegations of fraud and other crimes related to DOC operations and employees, and promote regulatory compliance for both the government and the grantees.

• All NOAA grant agreements include provisions for OIG access to records.
Grant Compliance Issues

• Biggest mistake: Not taking compliance seriously
• Rules with reason
• Corporate culture

• Professionalism
  – For-profit risks
  – Non-profit risks
• Hindrance or Help?
  – Boundaries
  – Keeping the doors open
  – Keeping me away
  – Employee retention

**Bottom Line:**
Compliance is good business
What You Should Know

• Every submission is a claim of truth made to a government official
  – Grant application and amendments
  – Bills, Vouchers or Invoices
  – Periodic performance and financial reports or certifications

• Every time you request payment, it is certifying you are in compliance with all material terms and conditions of the grant
Why You Should Care
Consequences of Non-compliance

• Administrative sanctions
  – Reduction in payments; recovery actions & penalties
  – Termination or Restructuring of Grant
• Suspension and Debarment
• Corrective action plans and forced compliance plans
• PFCRA or CMP remedies
• Criminal and Civil Penalties
  – Parallel proceedings – Personal liability possible.
  – Civil False Claims – treble damages + fines for each false claim
Recognizing Risk
Most Common Compliance Risk Issues

• Policies and procedures inadequate or nonexistent
• Inadequate accounting system to assemble, analyze, classify, record, manage and report on costs and assets
  – No ability to track costs by job or order – no separate financial administration for each award (i.e., commingling costs)
  – Difficult to audit, records messy or missing; unnecessarily complex accounting transactions or moving of money (adjusting entries)
  – Contentious or unusual accounting practices
  – No original receipts or original source records to support claimed costs
  – Cash transactions not well documented; many cash deposits
  – Records retention; photocopies instead of originals
  – Losses on commercial contracts; low number of bidders; cost shifting
Recognizing Risk

Most Common Compliance Risk Issues

- Costs that are not allowable, allocable, and/or reasonable
- Labor Charging
  - Direct v. Indirect Labor Costs and associated burden
  - Allocation when an employee worked on more than one project
  - Consistent with Approved Grant Budget
- Lack of subrecipient monitoring – no flow-down
- No segregation of duties
- Travel documentation inadequate
- Cost-sharing between projects or related entities
- Violations of institutional conflict of interest rules
- Residual funds – accounting and disposition
What is Grant Fraud?

An act of deceit, trickery or deliberate neglect, committed by a federal funding recipient against the funding agency for the purpose of gaining something of value.

One or more of the following acts has usually occurred:

– Misappropriation of federal funds or property
– Deliberate neglect of grant rules and guidelines
– Deliberate falsification of information
Nature of Grant Fraud

– May be programmatic, financial or both

– May be hidden, discreet or completely overt

– May involve a large OR small portion of an award

– May involve a conspiracy between subcontractors/subgrantees and/or government officials

– May be a one-time incident or ongoing matter
What Fraud Looks Like

- Encompasses theft, embezzlement, false or illegal commissions, kickbacks, false statements, false claims, collusive arrangements, and similar devices.
- Creating Fictitious Records
- Forgery
- Diverting Funds
- Double billing
What Fraud Looks Like

- Inflating enrollment and attendance records
- Fees for non-existent consulting services
  - Issuing checks payable to friends or relatives
- Submitting invoices for personal expenses
- False statements on grant application
- Using funds for unintended purposes
- Not providing services
- Falsifying research/data
What Fraud Looks Like

Grantee Employees
• Submitting false claims in travel vouchers/cost reports
• Using credit cards for personal use
• Diverting funds to phantom companies
• Kickbacks – Conflict of Interest and Self-Dealing
Investigation Examples

• A grant recipient was convicted for misapplying approximately $500,000 of grant funds to pay for personal expenses, including rent, home renovations, cleaning services, restaurant meals, and miscellaneous household items.

• Four officials of a grantee were convicted of fraud, conspiracy and money laundering after converting nearly $800,000 to their personal use.
Investigation Examples

- A NOAA grantee used about 55% of the total grant to buy, among other things, methamphetamines and a Rolex watch. The one-year grant was for developing a program to train on new fishing techniques.

- The Controller of a grantee embezzled grant funds from his employer by contracting out unnecessary construction services to a company a co-conspirator owned, and who kicked back a portion of the proceeds.

- A grantee shifted rent expenses for a related private company to make it appear costs were for the grantee.

- A grantee disguised hockey and baseball season tickets by breaking up the costs in the accounting records – submaterial costs.
Compliance Aimed at a Triangle

The Fraud Triangle

• **Incentive/Pressure.** Pressure, such as a financial need, is the “motive” for committing the fraud. Examples: meeting expectations in an economic downturn or a gambling problem.

• **Rationalization.** The person frequently rationalizes the fraud - “I’ll pay the money back”, “They will never miss the funds”, “They don’t pay me enough”, or “I won’t get caught.”

• **Opportunity.** The person committing the fraud sees an internal control weakness and, believing no one will notice if funds are taken, begins the fraud with a small amount of money, which grows over time.
Control Environment

• **Management’s philosophy and operating style**
  – No interest in managing fraud risk from the top – poor design
  – Decentralized mgmt without monitoring
  – No prior audits; audit firm collusion; evasive audit answers
  – Failure to act on complaints
  – Poor timekeeping systems (often intentional)

• **Organizational structure**
  – One person in control; no separation of duties
  – High turnover
  – Lack of training staff, vague work assignments

• **Personnel policies and practices**
  – Missing or incomplete control policies
  – Reality of their actual practice is not consistent with policies
Myth About Fraud - #1

- Only certain types of people will commit fraud......
And........

• Certain types of people will NOT commit fraud......
Who Commits Fraud?
Profile of Perpetrators of Fraud

- Older
- Church Attendance
- Stable Family
- Good Mental Health
- High Self-esteem
- Outgoing, charismatic
- Trusted
The Perpetrators - Age

• 2008 Study by Association of Certified Fraud Examiners found more than half of fraud cases in study involved a fraudster over the age of 40, and over one-third of the schemes were perpetrated by individuals between the ages of 41 and 50.
The Perpetrators
Age of Perpetrator — Median Loss

©2008 by the Association of Certified Fraud Examiners, Inc.
The Perpetrators

Tenure of Perpetrator — Frequency and Median Loss

©2008 by the Association of Certified Fraud Examiners, Inc.
The Perpetrators
Position of Perpetrator - Frequency

- Employee: 39.7% (2008), 41.2% (2006)
- Manager: 37.1% (2008), 39.5% (2006)
- Owner / Executive: 23.3% (2008), 19.3% (2006)

©2008 by the Association of Certified Fraud Examiners, Inc.
The Perpetrators
Education of Perpetrator – Median Loss

©2008 by the Association of Certified Fraud Examiners, Inc.
The Perpetrators
Education of Perpetrator – Frequency

©2008 by the Association of Certified Fraud Examiners, Inc.
Myth - #2

- Fraud is not material.
Fact

- Fraud Grows.... Consistently amounting to 7 to 10% - as high as 20% in some settings.
Myth #3

• Fraud is well concealed and too hard to detect
Myth # 4

• Auditors[Project Officers/Grant Managers] can’t detect fraud.

• You are on the front line of defense against fraud.
Playing it Safe

• Follow government rules, regulations and guidelines

• Act in good faith

• Ask questions - do not assume the answers

• Report accurate information

• Promote efficiency, honesty and professionalism

• Maintain fraud prevention refresher training

• Provide employees with a copy of contracting rules and regulations
Playing it Safe “Do’s”

• Avoid “gray areas” or risky situations with subcontractors
• Require full disclosure from employees and subcontractors
• Reward employees for identifying project weaknesses, waste, fraud and abuse
• Stay organized
• Report any problems timely and with full disclosure
• Communicate openly and often with your agency representative
Playing it Safe
“Don’ts”

- Double billing
- Inflated billing
- Poor accounting system
- Deliberate “accounting error”
- Deliberate product overage
- Product substitution
- Shifting costs often from one category or cost account to another without approval
- Fail to maintain adequate internal controls
Playing it Safe
“Don’ts”

• Embezzlement of project funds or equipment

• Misappropriation of project funds or equipment

• Deliberate waste of project funds, equipment and resources

• Unauthorized travel costs

• Conflicts of interest

• Less than arms length transactions

• Use of fictitious vendors

• Falsify time & attendance records
Playing it Safe
“Don’ts”

• Co-mingle project funds

• Give control of ASAP to the wrong person

• Alter or destroy documents

• Mislead government contracting/program officials

• Mislead auditors/inspectors

• Mislead your employees
The Golden Rule...

“The Golden Rule of Fraud Prevention”

WHEN IN DOUBT....DON’T DO IT.

Call your agency representative for appropriate guidance.
Please Contact Us

We want to hear ANY CONCERNS you may have regarding grant and procurement recipients or other Commerce program or employee fraud – lying, stealing and cheating.

– We DO NOT require that you detect evidence of a crime.

– We DO NOT require that there be a specific allegation.

– If you have suspicions….please contact us.
Legal Protections - Employees

Department Administrative Order (DAO) 207-10

• Requires employees to report to the OIG any information indicating possible existence of: any violation of law, rules or regulations, mismanagement, gross waste of funds, conflicts of interest, standards of conduct.

Government-wide Standards of Ethical Conduct, 5 CFR Section 2635.101(b)(11)

• “Employees shall disclose waste, fraud, abuse and corruption to appropriate authorities.”
Whistleblower Protections

**Whistleblower Protection Act of 1989**

**IG Act Section 7(c)**

- Federal employees may not be retaliated against or harassed by management for reporting information regarding potential crimes, frauds or violations of law to the OIG.

- A federal agency violates the Whistleblower Protection Act if it takes or fails to take (or threatens to take or fail to take) a personnel action with respect to any employee or applicant because of any disclosure of information by the employee or applicant that he or she reasonably believes evidences a violation of a law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.
The Recovery Act and various other statutes provides explicit protections for *non-federal whistleblowers*. These protections apply to all contractor and grantee staff working on Recovery Act awards or other types of contracts or grants. The laws prohibit recipients from discharging, demoting or discriminating against any employee for disclosing any concern to their supervisor, the head of a federal agency or his/her representatives, or the OIG, information that the employee believes is evidence of:

- Gross mismanagement or waste of grant or contract funds.
- Danger to public health or safety related to the use of funds.
- Abuse of authority related to the implementation or use of funds.
- Violation of law, rule or regulation related to an agency contract or grant awarded or issued related to funds.
Contact Information

OIG HOTLINE
Phone: (800) 424-5197
Fax: (202) 482-2803
Email: hotline@oig.doc.gov

U.S. Department of Commerce
Office of Inspector General
Office of Investigations

Scott McLeod
Special Agent
(303) 312-7667
smcleod@oig.doc.gov

For more information please visit our website
www.oig.doc.gov
Grant Fraud Awareness

Knowing Your Risks and Responsibilities

William Tokash
Special Agent, CFE

U.S. Department of Commerce
Office of Inspector General

May 5, 2015
Silver Spring, MD
Overview

- Department of Commerce Office of Inspector General
- What is Grant Fraud
- Types of Grant Fraud
- Case Examples
- How to Stay out of Trouble: Do’s and Don’ts
- Whistleblower Protection
- Consequences
Authorized by the 1978 IG Act

Investigative jurisdiction includes all funding, programs and employees of DOC to include all bureaus

- Independent Investigative Agency
- Federal Law Enforcement Officers
- Investigative Attorneys
- Auditors

Agents:
- Conduct Independent Investigations
What We Investigate

- Grant Fraud
- Contract Fraud
- Antitrust Violations
- Embezzlement
- Theft
- Conflicts of Interest
- Bribery/Kickbacks
- False Claims
- False Statements/Certifications
- Bank Fraud
- Money Laundering
- Employee Misconduct
What is Grant Fraud?

“An act of deceit, trickery or deliberate neglect, committed by a federal funding recipient against the funding agency for the purpose of gaining something of value.”

- Lying…Cheating…Stealing

One or more of the following acts has usually occurred:

- Conflict of Interest
- Lying/Misappropriation of Funds
- Theft
Nature of Grant Fraud

- May be programmatic, financial, or both
- May be hidden, discreet, or completely overt
- May involve a large OR small portion of an award
- May involve a conspiracy
  - subcontractors/subgrantees and/or government officials
- May be a one-time incident or ongoing matter
Process Safeguards

- Grantee’s Internal Controls
- Grant Management / Desk Audit
- Grantor Monitoring
- OIG Audits
- A-133 / Single Audit Act
- Public Availability of Reports
Who Commits Grant Fraud?

- Recipients
  - Company Officers
  - Business Partners
  - Board Members
- Employees
- Contractors/Subcontractors
- Consultants
Conflicts of Interest

- Grantees are required to use federal funds in the best interest of their program and these decisions must be free of undisclosed personal or organizational conflicts of interest—both in appearance and fact.

- The typical issues in this area include:
  - Less than Arms-Length or Related Party Transactions
  - Sub Grant Award Decisions and Vendor Selections
  - Consultants
“Lying” or Failing to Properly Support

- Grant Agreement
  - Legally Binding
  - Grantees Obligated to use funds as outlined in the agreement
  - To act with integrity when applying for and reporting their actual use of funds
  - Grantees to track the use of funds and maintain adequate supporting documentation

- The typical issues in this area include:
  - Matching Funds
  - Labor Hours/Wages
  - Indirect Cost Rates
  - Redirecting Funds
  - False Statements
Theft

- Most Common
- Embezzlement of Funds
- Cost Reimbursement Schemes
- Weak or Lack of Internal Controls
- “Profit” Not Allowed
• A NIST Advanced Technology Program recipient was convicted for misapplying approximately $500,000 of grant funds to pay for personal expenses, including rent, home renovations, cleaning services, restaurant meals, and miscellaneous household items.

• Four officials of an EDA Revolving Loan Fund program were convicted of fraud, conspiracy and money laundering after converting nearly $800,000 to their personal use.
A NOAA grantee used about 55% of the total grant to buy, among other things, methamphetamines and a Rolex watch. The one-year grant was for developing a small boat tuna pole and line training program to train native Hawaiian people in fishing techniques.

- The Controller of a grantee embezzled grant funds from his employer by contracting out unnecessary construction services to a company a co-conspirator owned, and who kicked back a portion of the proceeds. The controller paid these through spare company checks using a check protector.
- A grantee shifted rent expenses for a related private company to make it appear costs were for the grantee.
- A grantee disguised hockey and baseball season tickets by breaking up the costs in the accounting records – submaterial costs
“Do”

TIPS FOR KEEPING IT SAFE

- Avoid “Grey Areas”
- Require Full Disclosure
- Reward for Reporting
  - Fraud/Waste/Abuse
- Stay Organized
- Report Problems
- Communicate Openly
- Follow Government Rules, Regulations and Guidelines
- Act in Good Faith
- Ask Questions
- Report Accurate Information
- Promote Efficiency, Honesty, and Professionalism
- Fraud Awareness
“Don’t”

POST-AWARD
THINGS NOT TO DO

- Embezzlement
- Misappropriation
- Deliberate Waste
- Unauthorized Costs
- Conflicts of Interest
- Fictitious Vendors
- Falsify Records
The Recovery Act provides explicit protections for non-federal whistleblowers. These protections apply to all contractor and grantee staff working on Recovery Act awards. The Act prohibits funding recipients from discharging, demoting or discriminating against any employee for disclosing any concern to their supervisor, the head of a federal agency or his/her representatives, or the OIG information that the employee believes is evidence of:

- Gross mismanagement or waste of grant or contract funds.
- Danger to public health or safety related to the use of funds.
- Abuse of authority related to the implementation or use of funds.
- Violation of law, rule or regulation related to an agency contract or grant awarded or issued related to funds.
Consequences

- **Program Impairment / Failure**
- **Administrative**
  - Cancel awards
  - Recover funds
  - Withhold future funds
  - Suspension & Debarment
- **Civil False Claims Act…Treble Damages**
- **Criminal**
  - Prison
  - Fines & Restitution
  - Asset seizure
Summary

- Department of Commerce Office of Inspector General
- What is Grant Fraud
- Types of Grant Fraud
- Case Examples
- How to Stay out of Trouble: Do’s and Don’ts
- Whistleblower Protection
- Consequences
Please be on the lookout for...

ANYTHING that indicates fraud, waste, or abuse
Contact Information

**OIG HOTLINE**
Phone: (800) 424-5497
Fax: (202) 482-2803
Email: hotline@oig.doc.gov

U.S. Department of Commerce
Office of Inspector General
Office of Investigations

William Tokash
Special Agent
(202) 482-7481
wtokash@oig.doc.gov

For more information please visit our website
www.oig.doc.gov

11 May 2015