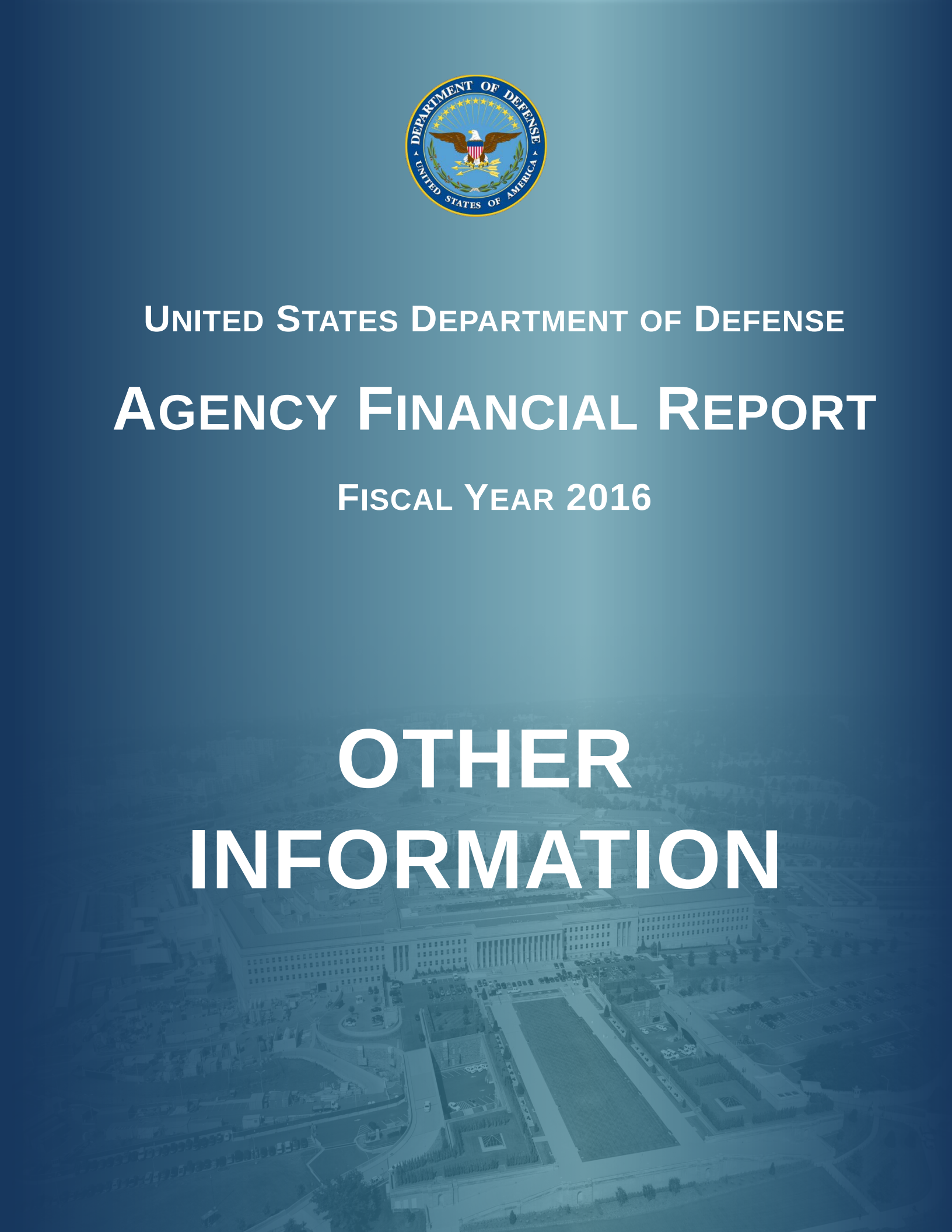
UNITED STATES DEPARTMENT OF DEFENSE

AGENCY FINANCIAL REPORT

FISCAL YEAR 2016

OTHER INFORMATION



Alaska Army National Guard Soldiers with B Company, 1st Battalion (Airborne),143rd Infantry Regiment, jump out of a UH-60 Black Hawk for the unit's final jump before they retire their airborne status, Aug. 5, 2016 at Joint Base Elmendorf-Richardson, Alaska. The Soldiers will remain in Alaska but fall under the 1st Battalion, 297th Infantry Regiment.

U.S. Air Force photo by Senior Airman James Richardson

160806-N-ZE250-245MEDITERRANEAN SEA (Aug. 6, 2016) - USS Carney (DDG 64) conducts a replenishment-at-sea with the Military Sealift Command fleet replenishment oiler USNS Big Horn (T-AO-198) and USS Wasp (LHD 1) in the Mediterranean Sea Aug. 6, 2016. Carney, an Arleigh Burke-class guided-missile destroyer, forward-deployed to Rota, Spain, is conducting a routine patrol in the U.S. 6th fleet area of operations in support of U.S. national security interests in Europe.

U.S. Navy photo by Mass Communication Specialist 3rd Class Weston Jones/Released)

OTHER INFORMATION
MANAGERS' INTERNAL CONTROL PROGRAM

The Department's management has a fundamental responsibility to develop and maintain effective internal controls to ensure federal programs operate and federal resources are used efficiently and effectively to achieve desired objectives. As discussed in the Internal Controls section of this report, managers throughout the Department are accountable for ensuring effective internal controls in their areas of responsibility. All DoD Components are required to establish and assess internal controls for financial reporting, mission-essential operations, and financial management systems.

Management-identified weaknesses are determined by assessing internal controls, as required by the Federal Managers' Financial Integrity Act of 1982 (*FMFIA*), the Federal Financial Management Improvement Act of 1996 (*FFMIA*), and Office of Management and Budget *(OMB) Circular No. A-123*, and fall into one of the following categories:

1. FMFIA Section 2, Financial Reporting Material Weaknesses (see Table 2a).
2. FMFIA Section 2, Non-Financial Operations Material Weaknesses (see Table 2b).
3. FMFIA Section 4, Financial System Nonconformance Weaknesses (see Table 2c).
4. FFMIA, Compliance with Section 803(a), FFMIA (see Table 3).

From left to right, Machinist Mate 1st Class Micah Patterson, Boatswains Mate 1st Class Stephen Wodraska, Engineman 2nd Class Richard Meyer, Mineman 1st Class Coy Tully and Mineman 3rd Class Pete Calvert, assigned to Commander, Task Group 56.1, launch a MK 18 MOD 2 unmanned underwater vehicle from a rigid-hull inflatable boat during Squadex 2016. Squadex 2016 demonstrates U.S./U.K. mine detection capabilities in the U.S. 5th Fleet area of operations.

U.S. Navy Combat Camera photo by Mass Communication Specialist 1st Class Blake Midnight

Summary of DoD Inspector General Identified Material Weaknesses in Internal Controls over Financial Reporting

Table 1 lists the DoD Inspector General (IG) - identified 13 areas of material weakness in the Department's financial statement reporting.

Table 1. Summary of Financial Statement Audit						
Audit Opinion: Disclaimer						
Restatement: Yes						
Areas of Material Weakness		**Beginning Balance**	**New**	**Resolved**	**Consolidated**	**Ending Balance**
1	Accounts Payable	1				1
2	Accounting Entries	1				1
3	Environmental Liabilities	1				1
4	Government Property in Possession of Contractors	1				1
5	Intragovernmental Eliminations	1				1
6	Operating Materials and Supplies	1				1
7	Reconciliation of Net Cost of Operations to Budget	1				1
8	Statement of Net Cost	1				1
9	Financial Management Systems	1				1
10	Fund Balance with Treasury	1				1
11	General Property, Plant & Equipment	1				1
12	Inventory	1				1
13	Accounts Receivable	1				1
	Total Material Weaknesses	**13**				**13**

Summary of Management Assurances

1. FMFIA Section 2, Financial Reporting Material Weaknesses. Under the oversight of the DoD Financial Improvement Audit Readiness (FIAR) Governance Board, discussed in the *FIAR Plan Status Report*, the Department's assessment of the effectiveness of its internal controls over financial reporting identified 44 material weaknesses in FY 2016.

Table 2 lists the material weaknesses in internal controls over financial reporting, captured by end-to-end process and the assessable unit for the material weakness, and incorporates changes from the weaknesses reported in the FY 2015 Agency Financial Report.

Table 2. Effectiveness of Internal Controls over Financial Reporting (FMFIA Section 2)								
Statement of Assurance: No Assurance								
End-to-End Process	**Areas of Material Weakness**	**FY 2015 Ending Balance**	**Revised FY 2016 Beginning Balance[1]**	**New**	**Resolved**	**Consolidated**	**Reassessed**	**FY 2016 Ending Balance**
Budget-to-Report	Fund Balance with Treasury (FBWT)	1	3					3
	Financial Reporting Compilation	1	6					6
Hire-to-Retire	Health Care Liabilities	1	2					2
	Civilian Pay	1	3			(1)		2
	Military Pay	1	4					4
Order-to-Cash	Accounts Receivable - Public	1	2			(1)		1
Procure-to-Pay	Contract/Vendor Pay	1	4				3	7
	Reimbursable Work Orders (Budgetary)	1	3					3
	Transportation of Things	1	2					2
	Transportation of People[2]	1	2				(2)	0
Acquire-to-Retire	Equipment Assets	1	1	1				2
	Real Property Assets	1	2					2
	Environmental Liabilities	1	2					2
	Government Furnished Property (GFP)[3]	-	0				1	1
	Internal Use Software (IUS)[4]	-	0				1	1
Plan-to-Stock	Inventory	1	4					4
	Operating Materials & Supplies (OM&S)	1	3					3
	Military Standard Requisitioning and Issue Procedures (Requisitioning Procedures)	1	1					1
Total Financial Reporting Material Weaknesses		**16**	**44**	**1**		**(2)[5]**	**3**	**46**

[1] In FY2015 the Department reported material weaknesses in seventeen areas/assessable units. The total weaknesses in all areas were forty-four. The FY2016 beginning balance was updated to reflect the individual count of material weaknesses for each area of material weakness.
[2] Transportation of People is not material to the Department and is no longer reported as a Department-wide area of material weakness.
[3] GFP was previously reported as an Internal Controls over Non-financial Operations (ICONO) material weakness, but was re-assessed in FY2016 as an Internal Controls over Financial Reporting (ICOFR) material weakness
[4] IUS was previously reported as an ICONO material weakness, but was re-assessed in FY2016 as an ICOFR material weakness
[5] In FY2016 the descriptions for Civilian Pay was consolidated into two overarching areas as the material weaknesses addressed similar challenges. The Department used the same approach and consolidated the descriptions for Accounts Receivable into one overarching area.

Table 2a provides a brief description of each of the material weaknesses in financial reporting, with corrective actions and the target correction year.

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting

	Areas of Material Weakness	Year Identified	DoD Components	Corrective Actions	Target Correction Year
1	Fund Balance with Treasury • Ineffective processes and controls to reconcile transactions posted to the Department's FBWT accounts with the Department of Treasury's records. • Collections and Disbursements are reported to Treasury but are not recorded in the Department's general ledger. • Ineffective processes to provide sufficient and accurate documentation to support FBWT transactions and reconciling items.	FY 2005	Department-wide	• Track and reconcile collection/disbursement activity from the core financial systems and associated feeder systems to the Department's general ledgers and to Treasury accounts. • Develop an auditable FBWT reconciliation process, to include implementation of internal controls that ensure reconciling differences are resolved in a timely and accurate manner. • Analyze and resolve transactions posted to budget clearing accounts ("suspense" accounts). • Analyze and resolve transactions reported on Treasury's Statement of Differences (e.g., deposit in-transit, Intra-Governmental Payment and Collection, and check issue differences). • Perform aging analysis and apply reconciliations backwards to any years possible. • Perform Statement on Standards for Attestation Engagements (SSAE) 16/ (SSAE) 18, Reporting on Controls on FBWT – Transaction Distribution which includes Defense Cash Accountability Systems.	FY 2019
2	Financial Reporting Compilation • Ineffective processes and controls to prepare accurate financial statements supported by general ledger balances	FY 2007	Department-wide	• Implement a Standard Financial Information Structure (SFIS) to standardize financial reporting that aligns with the Department's mission.	FY 2022

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	that align with Department strategic and performance plans, to include incorrect crosswalk and mapping of transactions to ensure completeness and accuracy of the financial reporting. • Inability to reconcile detail-level transactions with the general ledgers and to provide adequate supporting documentation for adjustment entries. • Accounting balances are unsupported due to inadequate financial management systems and related processes and procedures. • Inconsistency in documented processes and procedures for performing reconciliations and resolving differences and the actual processes in practice. • Lack of developed approach for performing reconciliations and retaining data for sensitive activities. • Inconsistent procedures for recording Journal Vouchers and Standard Business Transactions (SBT) and supporting documentation retention procedures poses a significant risk to producing accurate and complete financial statements and reports.			• Implement controls that ensure adequate documentation exists to validate and support journal entries. • Obtain population of feeder system data transactions and perform reconciliations from feeder systems to the financial statements. • Implement strategy for obtaining, reconciling and securely storing sensitive data. • Implement G-Invoicing, to include system change request requirements. • Implement the SFIS Standard Line of Accounting tools to validate financial data quality and to build and implement accounting system interfaces.	

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
3	Health Care Liabilities • Insufficient financial reporting and accounting for all health care costs and the lack of processes to reconcile Medical Expense and Performance Reporting System data. • Inability to obtain sufficient documentation from compliant transaction-based accounting systems to support the costs of direct care provided by DoD-managed military treatment facilities.	FY 2003	Department-wide	• Develop and implement methodology for patient itemized bills to address the auditor-identified weakness related to direct care. Itemized patient bills for all patients provided care will be attainable with the deployment of the new Electronic Health Record scheduled for full deployment across the Military Health Services by close of FY 2022.	FY 2022
4	Civilian Pay • Ineffective processes and controls to record civilian pay transactions and personnel actions in a timely, complete, and accurate manner, to include unreliable supporting documentation for personnel actions and timekeeping, and inadequate reconciliations between Defense Civilian Pay System (DCPS) and the general ledger. • No assessment of internal controls for time and attendance processes.	FY 2011	Department-wide	• Develop and implement controls to record personnel actions and timekeeping accurately and implement document retention policies and procedures to ensure that sufficient supporting documentation is available. • Develop and implement Complementary User Entity Controls identified in the DCPS SSAE16. • Develop and implement a methodology to reconcile DCPS to the general ledger. • Implement controls for general ledger posting procedures.	FY 2017

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
5	Military Pay • Ineffective processes and controls to record military pay transactions and personnel actions in a timely, complete, and accurate manner. • Lack of reconciliations between Defense Joint Military Pay System (DJMS) and the general ledger. • Unreliable and/or lack of supporting documentation for personnel actions. • Outdated military pay and financial management information technology systems lack modern capabilities to support required auditability framework. Current deficiencies require unsustainable manual activities to support auditability.	FY 2011	Department-wide	• Develop and implement a five year plan for an integrated pay and personnel system (IPPS), which will be designed to determine pay and entitlements, report ad hoc financial management data, and capture and store key supporting documents. • Implement reconciliations to address the completeness of data entered into DJMS.	FY 2021

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
6	Accounts Receivable - Public • Ineffective processes and controls to ensure complete and accurate recording of accounts receivable and the availability of sufficient documentation to support accounts receivable balances.	FY 2003	Department-wide	• Implement ERP systems to improve collections of public accounts receivables, aging of receivables, and minimize manual processes. • Implement process improvements, such as training, guidance, and policy changes. • Develop documentation in sufficient detail to address the edit checks and validations performed. • Utilize the Tri-Annual Review process to monitor the status of dormant reimbursable agreement receivables and unfilled orders. Reviews will evaluate timeliness, accuracy, and completeness for closeout when applicable.	FY 2017
7	Contract/Vendor Pay • Lack of standard data structure governing purchase request format prevents traceability and use of electronic transactions from initiation of funding through contract execution. • Need to implement standard processes for recording contract obligations electronically in financial systems. • Current environment does not enable match of award to accounting data for public transparency, (e.g., Data Act). • Lack of timely contract closeout and de-obligation of funds limits Department's access to capital.	FY 2003	Department-wide	• Publish DoD Instruction setting policies, procedures, and data standards for purchase requests. • Design and implement automated pre-award funds validation to ensure accounting systems can accurately record proposed contract award structure. • Scorecard all accounting and entitlement systems to track progress toward compliance with standard procedures. • Design and implement controls to ensure contract data can be accurately matched to recorded accounting data for public posting. • Develop department-wide contract closeout standard operating procedures to ensure financial systems are in balance and deobligation of funds occur returning	FY 2019

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	• Insufficient policies governing the recording of accruals related to contracts. • Inability to reconcile contract data to financial data. Unable to reconcile buyer and seller intragovernmental and intergovernmental transactions.			available funds back to programs in a timely manner. • Expand use of accrual recording based on Wide Area WorkFlow acceptance data to additional accounting systems. • Develop policies, procedures, and data standards for electronic intergovernmental/intragovernmental transactions. Pilot capability to obtain contract source data and source documentation for reconciliations to the financial records.	
8	Reimbursable Work Orders • Lack of evidence of performance, acknowledgement of receipt of intragovernmental goods and services, and validity of open obligations. • Inability to verify the timely and accurate collection of disbursements and validate recorded reimbursable agreements meet the time, purpose, and amount criteria. • Components are unable to collect, exchange, and reconcile buyer and seller intragovernmental transactions, resulting in adjustments that cannot be verified or substantiated. In addition, Department procedures required that buyer-side transaction data be	FY 2011	Department-wide	• Treasury has identified G-Invoicing as a solution to intragovernmental transaction (IGT) differences and will develop an online portal for conducting Buy/Sell transactions, to manage the processing and approval of general terms and conditions (GT&C) Agreements, Orders, and Invoices. • Reporting entities will perform gap analysis on key processes, build and enter GT&C's agreements in G-Invoicing system. Participate in G-Invoicing training, and build orders in accordance with data standards. • Reporting entities will fund, design, and build all accounting system interfaces in alignment with Treasury's G-Invoicing release schedule. • Reporting entities and Defense Finance and Accounting Service (DFAS) will implement	FY 2019

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	forced to agree with seller-side transaction data without substantiating documentation or performing proper reconciliations.			training, guidance, and management oversight related to Tri-Annual Reviews and identify and implement standard enterprise reconciliations that provide for validation of the seller/buyer-side balances and input of supported journal vouchers for timing differences.	
9	Transportation of Things • Effective controls are not in place to prevent unauthorized use of Transportation Account Codes (TAC) or unauthorized shipments from occurring. • The Department does not have a centralized process to capture, retain, and retrieve transportation documentation, which is required to support Transportation of Things (ToT) transactions, management evaluation, and future examination / audits.	FY 2014	Department-wide	• Develop controls, processes, and policy and procedures for ToT. • Continue to identify and implement standard systems and processes across the transportation community for Third Party Payment System Freight, Defense Personal Property Program, and Transportation Working Capital Fund.	FY 2018

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
10	Equipment Assets • Processes and controls to account for the quantity and value of military and general equipment are not effective. • DoD has insufficient internal controls and supporting documentation requirements to ensure timely recording, relief and accuracy of Construction in Progress (CIP).	FY 2006	Department-wide	• Develop implementation guidance to determine the value of military and general equipment in accordance with the recently published accounting standard for reporting entities undergoing audit for the first time. • DoD Components are implementing a "go forward" approach for valuing military and general equipment and sustaining these values (including CIP) in accordance with Generally Accepted Accounting Principles (GAAP); as well as modifying the accountable systems of record (APSRs) to capture required data. • Update the DoD Financial Management Regulation (FMR) chapters for accounting for military and general equipment. • Validate asset listings and document process and control environments. • Apply controls and procedures to manage property accountability, including adequate documentation to support acquisition and disposal processes throughout the year. • Report quarterly on status of establishing accountable records for all capitalized equipment. • Continue to convene the General Equipment Working Group to highlight policy and guidance gaps impacting the valuation of General Equipment and use the working Group as a forum for sharing lessons learned.	FY 2022

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
				• Revise DoD Instruction 5000.64 to address internal control improvements over property accountability such as designating a Component Property Lead, annually assessing Accountable Property System of Record capabilities, new guidance for transfers and new guidance for "non fielded" property.	
11	Real Property Assets • Real property processes, controls and supporting documentation do not substantiate that (1) all existing assets are recorded in an APSR (2) all assets recorded in the APSR properly reflect DoD's legal interest in the asset, (3) all assets are properly valued and (4) all assets are appropriately presented and consistently reported in the financial statements. • DoD has insufficient internal controls and supporting documentation requirements to ensure timely recording, relief and accuracy of CIP and real property.	FY 2003	Department-wide	• Complete floor-to-book and book-to-floor baseline reconciliation of real property assets with adequate documentation to support existence and completeness and rights and obligations assertions. Document go-forward processes and control environment for all lifecycle processes to include, acquisition (and CIP), inventory, reconciliation with financial statements, and disposal. • Establish systems to properly account for and value real property assets, including CIP. • Implement periodic evaluations over the quality of real property data by making comparisons with physical assets and annual reconciliations.	FY 2017
12	Environmental Liabilities • Inability to provide assurance that clean-up costs for all of its ongoing, closed, and disposal operations are identified, consistently estimated, and appropriately reported. • Unable to consistently report environmental liability disclosures and	FY 2001	Department-wide	• Continue to implement new DoD strategy for achieving Environmental and Disposal Liabilities Audit Readiness, providing guidance on capturing the environmental liability universe, estimation and modeling practices for developing the cost estimates, documenting and supporting those estimates,	FY 2017

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	supporting documentation is not properly maintained and readily available for all environmental sites.			and roll-forward procedures for ensuring that estimates are up to date. • Implement business processes and controls to ensure transactions are recorded timely and accurately, and supporting documentation is retained and available. • Identify common practices associated with asset-related environmental liabilities (e.g., general equipment, real property), to fully identify the asset universe and consistently value the associated environmental disposal liabilities. • Develop documentation for EL cost estimating models (e.g., RACER) to validate cost estimating model inputs and algorithms, centralize common documentation where feasible, and provide guidance on how to assess reasonableness of estimates produced as compared to actual expenditures.	
13	Government Furnished Property Lack of guidance and training on required policies and procedures for appropriately managing property provided to contractors (this includes contractor acquired property (CAP) and GFP). As a result, DoD's accountability records are incomplete. Audit reports have consistently identified a lack of accountability for GFP and CAP.	FY 2011	Department-wide	• Components to continue to report quarterly on progress in establishing accountable records for all GFP assets, correcting policy deficiencies, and ensuring controls are in place when property is furnished on contracts. In addition, implement Contractor Acquired Property guidance for establishing accountability and valuation. • Continue to report quarterly on progress in establishing accountable records for all capitalized equipment,	FY 2017

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
				correcting policy deficiencies, and ensuring controls are in place when property is furnished or purchased through contracts. • Develop measures for components to follow in implementing property management policies, including the proper accountability for property provided to contractors. • Improve policy and guidance for GFP management and CAP delivery to ensure accurate accountability and financial reporting. • Analyze existing end to end business processes identifying opportunities to improve capture and sharing of electronic data. • Validate accountable property records and supporting documentation through existence and completeness testing.	
14	Internal Use Software • The Department has not properly addressed the management and financial reporting of IUS which is required by the Financial Management Regulation. DoD will not be able to pass audit without developing and implementing IUS guidance.	FY 2015	Department-wide	• Components to begin managing and reporting IUS as required in the draft DoD Instruction for IUS accountability. This includes the identification of accountable officers, the universe of IUS, and annual IUS inventory requirements. • Publish a new DoD Instruction addressing IUS accountability and accountability and management of IUS assets. • Continue to convene the IUS Working Group established to address prospective IUS accounting and accountability policy and implementation.	FY 2020

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
15	Inventory • DoD does not have sufficient policies and procedures in place to support inventory transactions and related journal vouchers (JV). • There is a lack of controls to provide assurance that inventory recorded in the financial statements exist and is complete. • There is a lack of clear audit trails to trace transactions from source documentation to the reported total dollar values on the Inventory line item on the financial statements. • Material-in-transit is reported at the summary level instead of detail level and there is a lack of adequate processes and controls to assure the amount reported is correct.	FY 2005	Department-wide	• Develop methodology and inventory condition code reports to support monthly JV related to inventory, including retention of supporting documentation for all inventory transactions and related JVs. • Ensure periodic inventories and reconciliation of inventory accounts to the systems of record is performed. • Implement methodology to value inventory in the absence of historical costs (for baseline of asset inventory). • Develop and implement processes and controls to support the valuation of inventory on a "go-forward" basis. • Modify systems to account for Material-in-transit at the detailed level.	FY 2017
16	Operating Materials & Supplies (OM&S) • Historical cost data is not maintained and therefore inventory values cannot be reported as required by GAAP. • Inability to perform and document annual physical inventories of OM&S and maintain clear audit trails to permit the tracing of transactions from source documentation. • Government-owned / Contractor managed and Government Furnished	FY 2005	Department-wide	• Develop and document adequate business and financial processes and controls to include establishing a baseline and "go forward" approach to track inventory values for newly acquired OM&S. • Develop interim and go forward auditable solutions for Government owned/Contractor managed and GFM inventories. • Identify and document the current inventory reconciliation processes,	FY 2019

Table 2a. FY 2016 Material Weaknesses in Internal Controls over Financial Reporting					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	Material (GFM) inventories are not accounted for in DoD accountable property systems.			including key controls and financial transactions.	
17	Military Standard Requisitioning and Issue Procedures (Requisitioning Procedures) • Bulk obligations are not reconciled to transaction level detail.	FY 2013	Navy	• Develop and implement process to reconcile bulk obligation data to detail execution level. • Ensure compliance with existing policy to integrate obligation requirements with the MILSTRIP Tri-Annual Review.	FY 2017

Gunner's Mate 2nd Class James Callison coils line aboard the guided-missile destroyer USS Momsen (DDG 92) during a replenishment-at-sea with the fleet replenishment oiler USNS Joshua Humphreys (T-AO 188). The guided-missile destroyers USS Spruance (DDG 111), USS Decatur (DDG 73- and Momsen are deployed in support of maritime security and stability in the Indo-Asia Pacific as part of a U.S. 3rd Fleet Pacific Surface Action Group (PAC SAG) under Commander, Destroyer Squadron (CDS) 31.

U.S. Navy photo by Mass Communication Specialist 1st Class Jay Pugh/Released

2. FMFIA SECTION 2, NON-FINANCIAL OPERATIONS MATERIAL WEAKNESSES. The DoD Components use an entity-wide, risk-based, self-assessment approach to establish and assess internal controls for mission-essential operations. The material weaknesses in operational areas are categorized in separate reporting categories.

Table 2b lists the FY 2016 material weaknesses in the internal controls over operations.

Table 2b. Effectiveness of Internal Controls over Non-Financial Operations (FMFIA Section 2)						
Statement of Assurance: Qualified						
Area of Material Weakness	FY 2015 Ending Balance	Revised FY 2016 Beginning Balance[6]	New	Resolved	Re-assessed	FY 2016 Ending Balance
Acquisition	1	2		(2)		0
Security	1	1			(1)	0
Information Technology	1	4		(4)		0
Comptroller and/or Resource Management	1	3		(2)		1
Contract Administration	1	3				3
Force Readiness	1	1	1			2
Personnel and/or Organizational Management	1	1				1
Government Furnished Property[7] (GFP)	1	1			(1)	0
Internal Use Software[8] (IUS)		1			(1)	0
Supply Operations	1	1				1
Total Operations Material Weaknesses	9	18	1	(8)	(3)	8

Table 2b-1 provides a brief description of each of the area of material weaknesses in internal controls over operations, the associated corrective action, and the target correction year.

Table 2b-1. FY 2016 Material Weaknesses in Internal Controls over Non-Financial Operations					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
1	<u>Comptroller and Resource Management</u> • Ineffective internal controls and management oversight for	FY2013	Department-wide	• Brief leadership, appoint and train staff, develop risk profiles, conduct initial, quarterly and annual	FY2018

[6] The FY2016 beginning balance was updated to reflect the individual count of material weakness for each area of material weakness from the prior year.
[7] GFP was previously reported as an ICONO material weakness, but was re-assessed in FY2016 as an ICOFR material weakness.
[8] IUS was previously reported as an ICONO material weakness, but was re-assessed in FY2016 as an ICOFR material weakness

Table 2b-1. FY 2016 Material Weaknesses in Internal Controls over Non-Financial Operations					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	processes such as management of improper payments and use of government travel charge cards, IUS, and property furnished to contractors			validation and assessment, and automate as appropriate. • Implement instructions from the October 2016 DoD memorandum "Preventing Travel Pay Improper Payments and Enforcing Recovery" including: (1) Implement sufficient controls to verify that all required receipts and substantiating documents are provided and uploaded into travel systems, (2) Verify that claimed amounts match documents and receipts, (3) Implement adequate segregation of duties in payment approvals, and (4) Maintain continuous monitoring over improper payments and take appropriate action to mitigate instances of improper payments.	
2	Contract Administration • The Department must strategically manage Services Acquisition (SA), define outcomes, and capture data to do so. • The Department continues to face challenges meeting fiscal year competition goals and needs to address ill-suited contract arrangements and utilize incentives. • The Acquisition workforce is not appropriately sized, trained, and equipped to meet the Department's needs.	FY 2009	Department-wide	• Continue to track and monitor training requirements for Acquisition workforce including new training for Mid/High Level Requirements and Contracting Professionals. • Continue to implement the April 2016 DoD publication, "Guidance on Using Incentive and Other Contract Types" when selecting and negotiating a contract type.	Reassessed annually based on incremental improvements
3	Force Readiness • There is a lack of diversity within the Sea, Air, and Land (SEAL) Special Operations Forces which indicates a	FY 2011	Department-wide	• Implement diversity outreach initiatives that will review outreach and awareness activities to ensure that the Special Operations Forces is recruiting candidates with	FY 2020

Table 2b-1. FY 2016 Material Weaknesses in Internal Controls over Non-Financial Operations					
	Areas of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	potential operational weakness. The Global War on Terrorism identified the need for an operational need for SEALs with diverse backgrounds. • Independent and internal reviews of DOD's nuclear enterprise identified problems and recommendations needed for a safe, reliable, and credible nuclear deterrent. These included internal control related items such as a need for increased managerial oversight, for an improved self-assessment program, for increased oversight capability, and for useful nuclear inspection reports. The reviews also made recommendations to address these problems.			diverse backgrounds and skills. • Develop corrective action plans that align with the recommendations from the independent reviews. • Track, monitor, and validate implementation of corrective actions.	
4	Personnel and Organizational Management • There are weaknesses in standard processes for the authorization of personnel actions and time and attendance controls.	FY 2009	Department-wide	• Identify gaps, develop and implement a plan to create and publish the necessary documents to address the gaps.	FY 2018
5	Supply Operations • Government Accountability Office (GAO) identified several Department-wide weaknesses in the areas of asset visibility, inventory management, and materiel distribution.	FY 2011	Department-wide	• Improve Supply Chain Management operations through better demand forecasting, asset visibility, and distribution processes.	Reassessed annually based on incremental improvements

3. FMFIA SECTION 4, FINANCIAL SYSTEM NONCONFORMANCE WEAKNESSES. The Department requires financial system conformance with federal requirements and reports. The Department reported one weakness that includes a wide range of pervasive problems related to financial systems.

Table 2c. Conformance with Financial Management System Requirements (FMFIA Section 4)						
Statement of Assurance: Systems do not conform to financial management system requirements						
Non-Conformances	**FY 2015 Ending Balance**	**Revised FY 2016 Beginning Balance [9]**	**New**	**Resolved**	**Reassessed**	**Ending Balance**
1. Financial Management Systems	1	4				4
Total System Conformance Material Weaknesses	**1**	**4**				**4**

Three MV-22B Osprey tiltrotor aircraft with Marine Medium Tiltrotor Squadron 262 (Reinforced), 31st Marine Expeditionary Unit, idle atop the flight deck of the USS Bonhomme Richard (LHD 6) during Valiant Shield 16 in the Commonwealth of the Northern Mariana Islands. Valiant Shield 16 is a biennial field training exercise designed to develop the integration of joint U.S. forces. The training enables real-world proficiency of joint forces to detect, locate, track and engage units – at sea, in the air, on land, and in cyberspace – to prepare for a range of possible military missions.

U.S. Marine Corps photo by Cpl. Samantha Villarreal/Released

[9] In FY2015 the Department reported system nonconformance in one assessable unit. The total weaknesses in this area were four. The FY2016 beginning balance was updated to reflect the individual count of material weaknesses for each area of material weakness.

Table 2c-1, below, provides the description and corrective action plan for the material weakness related to internal control over financial systems.

Table 2c-1. FY 2016 Internal Control over Financial Systems Material Weakness

	Area of Material Weakness	Year Identified	DoD Components	Corrective Actions	Target Correction Year
1	• Financial Management Systems: The Department's financial systems currently do not provide the capability to record financial transactions in compliance with FFMIA, current federal financial management requirements, applicable federal accounting standards, and the Treasury USSGL at the transaction level. • The Department's IT systems environment includes numerous legacy systems, core enterprise systems that support the major end-to-end processes, and nine Enterprise Resource Planning (ERP) systems. Most of the business legacy systems were designed to support functional purposes, such as human resource management, property management, and logistics management, and not originally for auditable financial statement reporting. The current systems environment is made up of many mixed (feeder and general ledger) systems that lack integration and are not in line with the Federal Information System Controls Audit Manual (FISCAM) requirements with regards to entity-level technology general controls, application-level general controls and automated application controls. • Inadequate configuration and user management of newly implemented systems with lack of proper design and effectiveness of internal controls for access, segregation of duties, configuration management, system interfaces and audit trails.	FY 2001	Department-wide	• Develop effective financial management systems processes throughout the Department, including ERPs and other core financial systems, and prepare a plan to correct or replace many of the mixed (feeder and general ledger) systems. • Continue pre-deployment testing of end-to-end financial management systems in order to make necessary system improvements towards FFMIA compliance. • Continue to evaluate and track CAPs to include completion of assessments of legacy financial management and critical feeder systems and required system change requests to accommodate related control deficiency remediation activities. • Identify systems that affect internal controls over financial reporting and financial statement audit readiness, develop systems documentation, test controls and supporting documentation transactions, and remediate deficiencies and weaknesses (which may require modifications to the systems) in preparation for audit or SSAE16.	FY 2017

Table 2c-1. FY 2016 Internal Control over Financial Systems Material Weakness					
	Area of Material Weakness	**Year Identified**	**DoD Components**	**Corrective Actions**	**Target Correction Year**
	• The Department has not fully defined and consistently implemented the full range of business systems modernization management controls. As a result, it may not be able to adequately ensure that its business system investments are the right solutions for addressing its business needs, as indicated by GAO 2015 High Risk report.				

Aviation Boatswain's Mate (Handling) Airman Nelson Lopez Delgado, from Havana, Cuba, prepares to lower the U.S. flag for evening colors on the Navy's only forward-deployed aircraft carrier, USS Ronald Reagan (CVN 76). During evening colors the U.S. flag is lowered at sunset each day while Ronald Reagan is in port. Ronald Reagan provides a combat-ready force, which protects and defends the collective maritime interests of the U.S. and its allies and partners in the Indo-Asia-Pacific region.

U.S. Navy photo by Mass Communication Specialist 2nd Class James Mullen/Released

FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT

The DoD IG and the audit agencies within the Military Services have reported on the Department's noncompliance with FFMIA. The Department's noncompliance is due to its reliance upon legacy financial management systems by the various Components. These legacy financial systems, for the most part, do not comply with the wide range of requirements for systems compliance, in accordance with FFMIA and therefore do not provide the necessary level of assurance that the core financial system data or the mixed systems information can be traced to source transactional documentation. Table 3 reflects the Department's compliance with FFMIA.

Table 3. Compliance with Federal Financial Management Improvement Act

Table 3. Compliance with Federal Financial Management Improvement Act		
	Agency	**Auditor**
1. System Requirements	Lack of substantial compliance noted	Lack of substantial compliance noted
2. Accounting Standards	Lack of substantial compliance noted	Lack of substantial compliance noted
3. U.S. Standard General Ledger at Transaction Level	Lack of substantial compliance noted	Lack of substantial compliance noted

Gas Turbine Systems Technician (Mechanical) 3rd Class Brandon Rasberry, from Humble, Texas, takes a fuel sample aboard USS Ross (DDG 71) during a replenishment at sea with the Military Sealift Command fleet replenishment oiler USNS Big Horn (T-AO 198) Aug. 1, 2016. Ross, an Arleigh Burke-class guided-missile destroyer, forward-deployed to Rota, Spain, is conducting naval operations in the U.S. 6th Fleet Area of Operations in support of U.S. national security interests in Europe and Africa.

U.S. Navy photo by Mass Communication Specialist 1st Class Theron J. Godbold/Released

IMPROPER PAYMENT AND PAYMENT RECAPTURE PROGRAMS

The Federal Improper Payments Coordination Act of 2015 amended the Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012 and earlier legislation affecting improper payments[10] and requires extension of the Do Not Pay Initiative and Departmental reporting of its data analytics performance. The intent is to ensure Federal and State Entities maintain strong financial management controls to better detect and prevent improper payments, and to report on these programs to the President and Congress in the annual Agency Financial Report. Amending legislation changed how the Department's improper payments and payment recapture programs are reported. The following subcategories are included in this section:

I. Risk Assessment
II. Statistical Sampling Process
III. Program Improper Payment Reporting
IV. Root Causes of Errors
V. Corrective Actions
VI. Internal Controls over Payments
VII. Accountability
VIII. Agency Information Systems and Other Infrastructure
IX. Statutory and Regulatory Barriers
X. Payment Recapture Audit Reporting
XI. Disposition of Funds Recaptured Reporting
XII. Aging of Outstanding Overpayments Reporting
XIII. Additional Information
XIV. Agency Reduction of Improper Payments with the Do Not Pay Initiative

The Department reports improper payments for the following six programs:

1. Military Health Benefits – Disbursed by Treasury for the Defense Health Agency (DHA)
2. Military Pay – Disbursed by DFAS
3. Civilian Pay – Disbursed by DFAS
4. Commercial Pay (vendor and contract payments) – Disbursed by DFAS, Navy, and U.S. Army Corps of Engineers (USACE)
5. Military Retiree and Annuitant Benefit Payments – Disbursed by DFAS
6. Travel Pay – Disbursed by DFAS, Navy, and USACE

The DFAS, USACE, and DHA are the primary disbursing Components within the Department.

[10] *Improper Payments Information Act of 2002* (IPIA), as amended by *The Improper Payments Elimination and Recovery Act of 2010* (IPERA) and *The Improper Payments Elimination and Recovery Improvement Act of 2012* (IPERIA)

I. Risk Assessment

DFAS. The DFAS risk assessment for disbursements uses established criteria contained in the *OMB Circular No. A-123, Appendix C*. DFAS monitors changes in programs associated with OMB-mandated criteria (for example, a large increase in annual outlays, regulatory changes, or newly-established programs) to identify unfavorable trends and allow for early implementation of corrective actions.

USACE. The USACE risk assessments for travel and commercial payments address the effectiveness of internal controls, such as prepayment reviews, to prevent improper payments as well as system weaknesses identified internally or externally by external audit activities. The U.S. Corps of Engineers Financial Management System (CEFMS) provides internal system standards that adhere to U.S. GAAP, as well as process controls that provide the safeguards to monitor and ensure that prepayment examination requirements are met. The USACE also monitors changes in programs to track trends and implement corrective actions, as necessary.

DHA. The DHA risk assessment process is managed through an external independent contractor (EIC) to provide independent, impartial review of reimbursements and claims processing procedures used by DHA's purchased-care contractors. The EIC identifies improper payments resulting from the contractors' noncompliance with The Military Health Care System (collectively referred to as TRICARE in this report) benefit and/or reimbursement policies, regulations, and contract requirements. The risk level of programs is evaluated based on results of these compliance reviews.

Navy. The Department of the Navy's Office of Financial Operations is updating guidance to reflect recent changes resulting from IPIA amendments (IPERA and IPERIA) and updates to OMB's Circular A-123, Appendix C. Communicating updated guidance to stakeholders will be accompanied with a more formal program governance structure, including the establishment of a program office and formal appointment of a Component Senior Accountable Official. A "Tone at the Top" memorandum for distribution is also being prepared for communication to all commanders and accountable officials, reflecting the Department of the Navy's commitment to good stewardship of taxpayer dollars and reminding appointing officials of their duty to hold accountable those responsible for certifying payments, as well as those which certifiers rely upon to make payments (e.g., Departmental Accountable Officials).

II. Statistical Sampling Process[11]

The primary disbursing Components use statistically valid sampling methods designed to meet or exceed OMB's requirements of a 90 percent confidence level and a margin of error of ±2.5 percent. By using these methods, disbursing Components are able to identify valid sample sizes and project improper payment percentages for the Department's improper payment programs. The smaller disbursing Components normally perform 100 percent post payment

[11] Refer to detail at *Under Secretary of Defense (Comptroller) > Financial Management > Reports* for Reporting Components Statistical Sampling Plans.

reviews or a full review of payments above a specific dollar threshold, with random sampling for lower-dollar payments. Updated sampling plans for DFAS Commercial Pay and DFAS Travel Pay were submitted to OMB for Fiscal Year (FY) 2016. In FY 2017 DFAS will address previous GAO recommendations by further updating its sampling plans for Travel Pay, Military Pay, and Civilian pay, changing each to a methodology that stratifies the populations by the dollar amount of the payment.

Military Health Benefits. The EIC compliance reviews include two sample types to measure improper payments: a payment sample (to ensure payment accuracy by identifying underpayment and overpayments) and a denied payment sample (to ensure proper claim denial). Payment samples are conducted as a stratified random sample based on paid amounts, while denied samples are conducted as a stratified random sample based on billed amounts.

- Payment Samples: Payment Samples for paid claims include between 4 and 12 strata, depending on the composition of the claims in the universe. Mathematical formulas are used to identify optimal strata boundary points, and sample sizes are calculated to yield an estimate with a minimum of 90 percent confidence and a margin of error of ±2.5 percent. All claims with a paid amount above a high-dollar threshold (i.e., $200,000) are reviewed, and claims with a paid amount below a $100 low-dollar threshold are excluded. The high-dollar thresholds may vary from contract to contract.
- Denied Payment Sample: Denied payment samples are limited to claims with $0 government payment. The denied payment sample is similar in design to the payment sample, but the denied sample is stratified based on billed amount because the paid amount for a denied claim is equal to $0. All claims with a billed amount above a high-dollar threshold (i.e., $200,000) are reviewed, and claims with a billed amount below a $100 low-dollar threshold are excluded. These thresholds may vary from contract to contract.

In addition, DHA conducts an internal statistically valid review of low-dollar claims excluded from the payment samples. Results from this internal review are combined with results from the EIC compliance reviews to arrive at an overall payment accuracy measurement for all DHA claims.

The DHA continually evaluates the accuracy and design of its sampling methodologies for all contracts and implements revisions, if warranted by the distribution of data within audit universes or the outcome of compliance reviews.

Military Pay. On a monthly basis, the Department statistically samples Military Pay accounts stratified by Active Duty (Army, Navy, Air Force, and Marine Corps) and Reserve Components (Army Reserve, Army National Guard, Navy Reserve, Air Force Reserve, Air National Guard, and Marine Corps Reserve). The Defense Management Data Center (DMDC) provides a sample of the total universe of military pay accounts for each branch and Component. DFAS reviews the pay accounts and provides annual estimates of improper payments.

Civilian Pay. On a monthly basis, DFAS statistically samples Civilian Pay accounts stratified by Army, Air Force, Navy/Marine Corps, and Defense Agencies. DMDC provides a sample of the total universe of civilian pay accounts, by payroll ID, for review. DFAS reviews the pay accounts and provides annual estimates of improper payments.

Commercial Pay. For FY 2016 nine contract and vendor pay systems[12] were identified as "at risk" of making improper payments based on historical post payment, self-identified reviews and the volume of outlays. These nine systems cover over 90 percent of the Commercial Pay program outlays.

DFAS designed its samples using a dollar-stratified sampling plan and the Neyman Allocation method. The Neyman Allocation method stratifies by dollar amount using financial data within each system and allocates to those strata. The overall variable sample size was calculated for the combined systems to produce a point estimate with a 95 percent confidence interval and a margin of error of ±2.5 percent. Samples were then randomly selected using the Statistical Package for the Social Sciences (SPSS) statistical software from the nine systems as a whole. Each invoice within each stratum had an equal probability of selection.

The sampling framework, designed by DFAS statisticians and reviewed by its Internal Review office, addressed GAO and DoD OIG audit recommendations. The sampling framework also was submitted to OMB, and no issues were noted.

Navy. The Navy compliance review includes contract and vendor payments computed in the Navy ERP, as well as two Commercial Bill Paying Offices overseas (Naples and Singapore). In FY 2017, Navy ERP will transition to DFAS for reporting.

USACE. The USACE post payment compliance reviews were conducted using a statistically valid, 95 percent confidence level and a margin of error of ±2.5 percent, sample taken from the entire USACE Commercial Pay universe. In addition, the USACE Finance Center (UFC) used prepayment controls, post payment contract audits, and data mining to prevent and identify improper payments in Commercial Pay.

Military Retiree and Annuitant Benefit Payments. On a monthly basis, DFAS statistically samples military retirement payments stratified by the retired and annuitant pay accounts. The review contains samples of: drilling reserve units, retiree offsets, survivor benefit plans, transfers to/from the Temporary Disability Retired List to the Permanent List, and Veterans Affairs offsets. Continuous random reviews are done for: Combat Related Special Compensation, Concurrent Receipt of Disability Payment, daily payroll accounts, newly established accounts, and other targeted areas.

[12] Computerized Accounts Payable System for Windows (CAPS-W), Defense Agencies Initiative (DAI), Enterprise Business System (EBS), General Funds Enterprise Business System (GFEBS), Integrated Accounts Payable System (IAPS), Mechanization of Contract Administrative Services (MOCAS), and One Pay (ONEPAY). In FY 2016, DFAS began reviewing the Defense Agency Accounting and Management System (DEAMS) and Navy Enterprise Resource Planning (NERP) (paid by DFAS).

Travel Pay

DFAS. DFAS uses an annual sampling plan stratified by Component for its Travel Pay reviews. Data is obtained through the Defense Technology Security Administration/Management Information System (DTSA/MIS) website, COGNOS, and the Rome Temporary Duty (TDY) database and used to produce monthly sample sets for review based on the annual plan. The annual sample size for each Component (Army, Navy, USMC, Air Force, and DoD Agencies for Defense Travel System (DTS); Active, Reserve, Casualty, Contingency, Civilian PCS, DoD Agencies, IMET, Military PCS, and Navy Reserve for Windows Integrated Automated Travel System (WinIATS)) is divided by 12 to obtain a monthly sample size. The Postpay Review & Analysis (PR&A) team statisticians select a random sample from each Component. The PR&A Travel Pay team reviews the samples to provide annual estimates of overpayments, provide error trends to the Services and Agencies, and recommend changes to regulations and travel pay systems. At the end of the fiscal year, PR&A statisticians use the monthly results to produce improper payment estimates, in accordance with OMB Circulars A-136 and A-123, IPIA, IPERA, and IPERIA, for each Component, DTS overall, WinIATS overall, and Travel Pay overall.

USACE. The UFC processes USACE travel payments using the CEFMS and WinIATS. The payment population includes both TDY and PCS travel voucher reimbursements. All PCS and TDY vouchers over $2,500 are 100 percent reviewed for accuracy. The remaining vouchers are statistically sampled at 95 percent confidence level and a margin of error of ±2.5 percent.

An F-22 Raptor, from Langley Air Force Base, Va., banks off after receiving fuel from a KC-135 Stratotanker over the Nevada Test and Training Range in a training sortie during Red Flag 16-3, July 21, 2016. During Red Flag 16-3, units from the U.S. Air Force, Marine Corps and Navy will work together to succeed in air, space and cyberspace.

U.S. Air Force photo by Senior Airman Jake Carter/Released

III. Program Improper Payment Reporting

Table 4 summarizes the Department's improper payment reduction outlook and total program outlays (prospective payments) from FY 2015 through FY 2019.

Table 4. Improper Payment Reduction Outlook ($ in millions)

Program or Activity	FY 2015 Outlays	FY 2015 IP %	FY 2015 IP	FY 2016 Outlays	FY 2016 IP %	FY 2016 IP	FY 2016 Over-payment	FY 2016 Under-payment	FY 2017 Est. Outlays	FY 2017 Est. IP %	FY 2017 Est. IP	FY 2018 Est. Outlays	FY 2018 Est. IP %	FY 2018 Est. IP	FY 2019 Est. Outlays	FY 2019 Est. IP %	FY 2019 Est. IP
Military Health Benefits [1, 2]	$19,700.00	0.80	$157.67	$20,461.50 [3]	0.74 [4]	$146.10 [5]	$121.60	$24.50	$20,870.70	1.75	$365.20	$21,663.80	1.75	$379.10	$22,465.30	1.75	$393.10
Military Pay [6]	$107,400.00	0.23	$242.90	$114,902.75	0.17	$196.23	$183.66	$12.57	$93,500.00	0.29	$271.20	$93,500.00	0.29	$271.20	$122,930.00	0.29	$356.50
Civilian Pay [6]	$56,600.00	0.10	$57.20	$58,088.10	0.10	$58.73	$58.73	$0.00	$56,500.00	0.17	$96.10	$56,500.00	0.17	$96.10	$59,600.00	0.17	$101.31
Military Retirement [6]	$59,300.00	0.04	$20.80	$59,931.73	0.02	$9.46	$8.92	$0.54	$44,100.00	0.04	$17.60	$44,100.00	0.04	$17.60	$60,930.00	0.04	$24.37
DoD Travel Pay [7]	$6,600.00	7.90	$521.47	$6,254.67	7.23	$451.99	$442.05	$9.94	$9,104.71	4.46	$406.07	$9,104.71	4.46	$406.07	$8,501.05	4.75	$403.80
DFAS Commercial Pay [6,8]	$287,800.00	0.09	$256.00	$248,536.45	0.04	$110.82	$110.82	$0.00	$384,700.00	0.03	$115.40	$384,700.00	0.03	$115.40	$287,800.00	0.03	$86.34
USACE Travel Pay	$170.00	0.02	$0.04	$188.00	0.20	$0.38	$0.38	$0.00	$180.00	0.17	$0.30	$180.00	0.17	$0.30	$180.00	0.17	$0.30
USACE Commercial	$18,200.00	0.00	$0.00	$18,158.00	0.00	$0.00	$0.00	$0.00	$18,200.00	0.00	$0.00	$18,200.00	0.00	$0.00	$18,200.00	0.00	$0.00
Navy ERP Commercial Pay [9]	$5,000.00	0.00	$0.00	$6,901.27	0.00	$0.00	$0.00	$0.00	$0.00	0.00	$0.00	$0.00	0.00	$0.00	$0.00	0.00	$0.00
Navy Commercial Bill Pay Office – Naples [10]	$0.00	0.00	$0.00	$472.03	0.01	$0.06	$0.00	$0.06	$472.00	0.01	$0.05	$472.00	0.01	$0.05	$472.00	0.01	$0.04

Note 1: DHA reports 12 months in arrears; therefore its FY 2016 reporting represents FY 2015 data.

Note 2: DHA uses 1.75% as its out-year target because that is the contractual performance standard. The FY 2017-2019 outlays estimates were calculated using the OMB CPI-U Annual Averages and Percent Change Table. As DHA reports 12 months in arrears, the FY 2016 CPI-U medical percent change was used to calculate the FY 2017 outlay estimates, while the FY 2017 and 2018 medical percent changes were used to calculate the FY 2018 and 2019 outlay estimates, respectively.

Note 3: Total outlays for DHA totaled $20,461,486,927. However, the IP % is based on $19,681,648,723. The difference in totals is the result of: 1) the TPharm quarterly 2015'05-2015'07 audit was not conducted due to system constraints (that have since been resolved); 2) the TPharm 2014'10-2015'09 low dollar audit was not conducted due to contractor's opposition to participate (which the agency is working to rectify); and 3) the ADDP semi-annual 2014'08-2015'01 audit was not conducted due to system constraints (that have since been resolved).

Note 4: The improper payment rate total of 0.74% does not represent a true statistical overall estimate for DHA due to three samples that were not conducted (specified in Note 3 above).

Note 5: The "FY2016 IP" total for DHA represents improper payment dollars extrapolated from actual audits. This number will not equal "FY2016 IP %" of "FY2016 Outlays" because the IP % was not applied to claims in samples that were not conducted (see Note 3 above). Also, the sum of paid dollars for individual audit universes will not equal the total FY outlays (see Appendix A for additional explanation).

Note 6: Out-year reduction targets for Mil Pay, Civ Pay, Mil Retirement, and DFAS Commercial Pay represent a continuation of the very low IP rates experienced in FY 2016.

Note 7: DFAS Travel Pay includes travel data for WinIATS processed and paid through DFAS and DTS for all services and Agencies. The review covered disbursed payments from July 2015 through June 2016.

Note 8: DFAS Commercial Pay review covered disbursed payments from July 2015 through June 2016 for the nine systems outlined in the risk assessment.

Note 9: Effective FY 2017, Navy ERP Commercial Pay will be transferred to DFAS.

Note 10: Navy Commercial Bill Pay Office – Naples began reviews and reporting in FY 2016. Navy Commercial Bill Pay Office – Singapore begins reviews and reporting in FY 2017.

IV. Root Causes of Errors

Table 5 summarizes the Department's improper payment root causes.

Table 5. Improper Payment Root Cause Category Matrix ($ in millions)

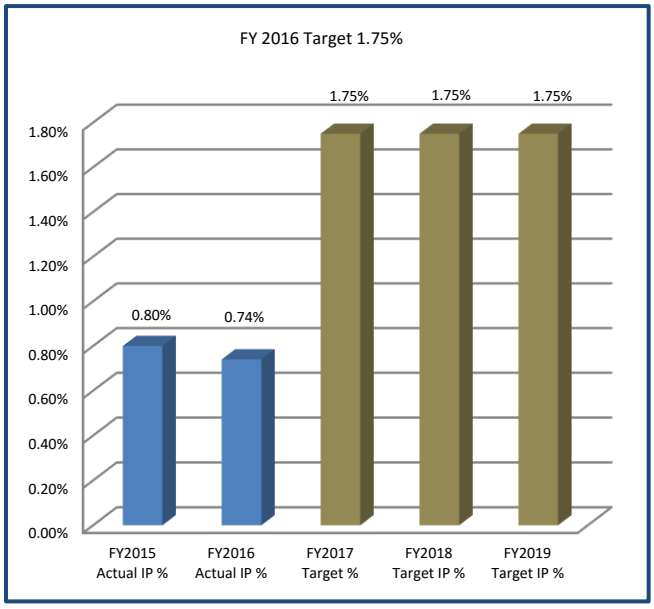
Reason for Improper Payment		*Military Pay*		*Civilian Pay*		*Retired Pay*		*Commercial Pay*		*Travel Pay*		USACE Travel Pay		DHA (Military Health Benefits)	
		Over-payment	Under-payment	Over-payment	Under-payment	Over-payment	Under-payment	Over-payment	Under-payment	Over-payment	Under-payment	Over-payment	Under-payment	Over-payment	Under-payment
Program Design or Structural Issue		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Inability to Authenticate Eligibility		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.12	$0.08
Failure to Verify:	Death Data	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Financial Data	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Excluded Party Data	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Prisoner Data	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Other Eligibility Data	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Administrative or Process Errors Made by:	Federal Agency	$183.66 [1]	$12.57 [1]	$58.73 [1]	$0.00	$0.64	$0.54	$110.82	$0.06	$252.18	$9.89	$0.00	$0.00	$0.00	$0.00
	State or Local Agency	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	Other Party	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Medical Necessity		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$3.13	$0.00
Insufficient Documentation to Determine		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$189.74	$0.00	$0.00	$0.00	$0.03	$0.00
Other Reason (a)		$0.00	$0.00	$0.00	$0.00	$8.28	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Other Reason (b)		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.13	$0.00	$0.00	$0.00	$0.00	$0.00
Other Reason (c)		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.05	$0.00	$0.00	$0.00	$0.00
Other Reason (d)		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.38	$0.00	$0.00	$0.00
Other Reason (e)		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$118.32	$24.42
TOTAL		**$183.66**	**$12.57**	**$58.73**	**$0.00**	**$8.92**	**$0.54**	**$110.82**	**$0.06**	**$442.05**	**$9.94**	**$0.38**	**$0.00**	**$121.60**	**$24.50**

(a) Notification of death after monthly payments disbursed for Military Retirees and Annuitants.
(b) Department of the Navy overpayments were primarily due to missing receipts.
(c) Department of Navy underpayments were due to miscalculation of travel entitlements.
(d) USACE overpayments result from erroneous TAO/CO Approval. USACE underpayments result from employee failures to claim authorized expenses.
(e) DHA reasons for overpayments and underpayments include: incorrect pricing, government pay miscalculation, cost/share deductible, procedure code errors, and payment omissions.
Note 1: The amounts reported have been recovered or a debt has been established for recovery.

Military Health Benefits

The projected FY 2016 error rate for military health benefits (MHB) improper payment is 0.74 percent.

Figure 19: Improper Payment Rate - Military Health Benefits



The DHA's purchased-care contracts are designed to include payment accuracy performance standards for processing MHB claims. Specifically, if improper payments exceed the payment accuracy performance standard, as stipulated in Military Health Care System policy manuals, or exceed more stringent purchased-care performance standards, the contractors are subject to financial penalties. Conversely, if the purchased-care contractor's improper payments fall below the DHA TRICARE policy requirement or unique contract performance standard(s), the purchased-care contractor may receive a financial incentive award.

Purchased-care contractor payment accuracy performance is analyzed during the EIC quarterly and semi-annual compliance reviews. In addition to these reviews, annual reviews are conducted on claims representing underwritten healthcare costs that are paid by the managed-care support contractors (MCSCs). Confirmed overpayments from annual audits are projected to the sample universe, and the MCSCs are liable for the total extrapolated error amount.

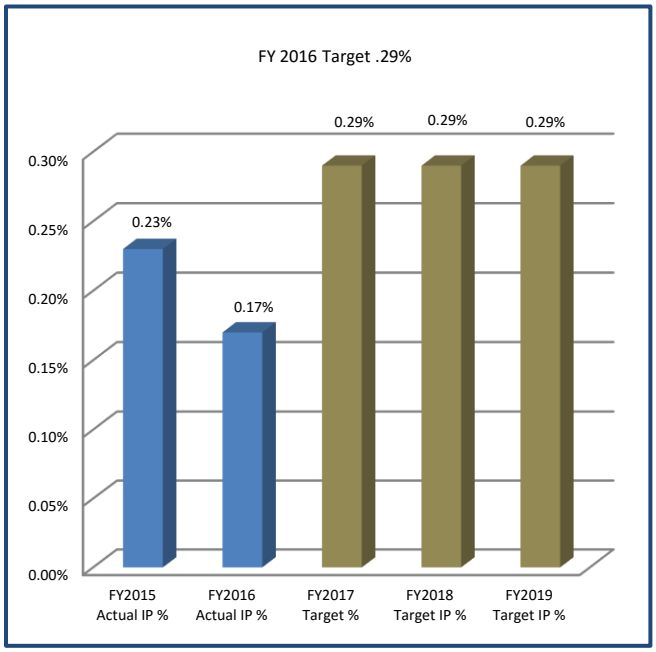
For the past several years, purchased-care contractors were held to payment accuracy performance standards with either contract financial penalties or incentives, depending on the contract type and requirement(s). This contract design encourages contractors to keep payment error rates as low as possible to avoid financial penalties, or to obtain increased contract financial incentives. Actual error rates have been consistently less than DHA's policy or contract performance standards. This contract design, combined with numerous pre- and post-payment controls, effectively curtails improper payments by the DHA's purchased-care contractors and ensures the Government's risk for improper payments in the MHB program is low.

In FY 2014, the formula used to calculate the DoD improper payment rate for the MHB program was changed. Specifically, the error rate was changed to calculate the error as a percent of dollars paid versus dollars billed. The errors identified in random samples were extrapolated using a weighted formula. Consequently, the FY 2014 error rate cannot be compared with previous years due to this change.

Root Causes. The primary reasons for payment errors in the MHB program for this reporting cycle are:

- Incorrect pricing of medical procedures and equipment, 32 percent;
- Lack of authorization or pre-authorization, required prior to receiving medical care, 18 percent;
- Other Health Insurance – Government Pay Miscalculated, 12 percent; and
- All other causes combined, 50 percent.

Figure 20: Improper Payment Rate - Military Pay



Military Pay. The Department projects a 0.17 percent error rate in FY 2016 Military Pay for improper payments based on review of trends in data from October 2015 to September 2016. Overpayments, which comprise 93 percent of the Military Pay improper payments, were scarcely found in statistical sampling, less than 0.005% percent, but primarily in debts established after a member has left the Military Service and through Active Duty debt collections reported by the Military Services.

Root Causes. The primary reason for recurring Military Pay errors is the units and service members untimely submittal of military pay documents for processing. Nearly 100 percent of the improper payments identified during this reporting period were recovered, or in the process of being recovered.

Military Pay improper payments typically result in incorrect entitlement allocation as described above. These entitlements are:

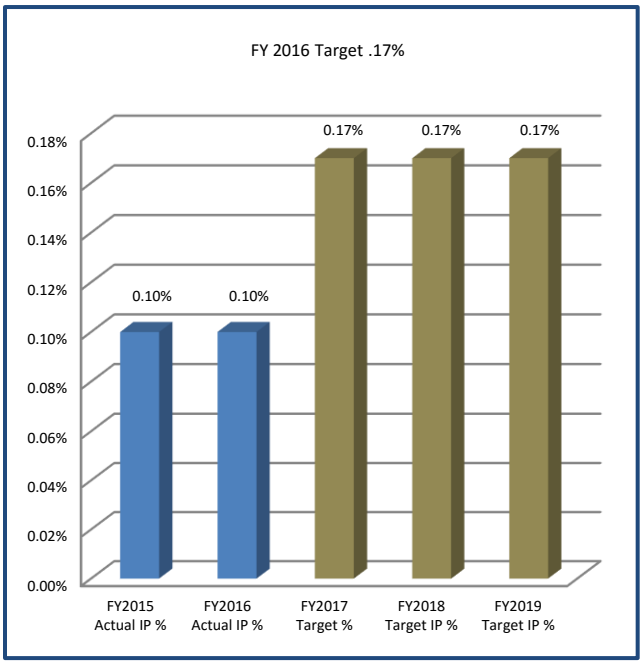
- Basic allowance for housing, 55 percent;
- Base pay for Active Duty and incorrect Active Duty pay for Reservists, 10.5 percent;
- Overseas housing allowance, 6 percent;
- Family separation allowance, Active and Reserve, 5.5 percent;
- Hostile fire/imminent danger pay, 5 percent; and
- Miscellaneous categories, including results from underpayments, account for 18 percent of all improper payments. Miscellaneous categories include over 25 different entitlements.

Civilian Pay. The Department projects a 0.10 percent error rate in FY 2016 for Civilian pay payments, primarily overpayments.

Root Causes. The Civilian Pay improper payments primarily were overpayments due to administrative errors caused by untimely or inaccurate entry of information into the pay systems. This is in part due to the high turnover rate of civilian payroll clerks. Improper payments identified include:

- Time and attendance, 49 percent;
- Overseas and other allowances, 28 percent; and
- Late personnel actions, 23 percent.

Figure 21: Improper Payment Rate - Civilian Pay



DCPS, like most government payroll systems, require time and attendance submissions occur prior to the end of the actual pay period to meet processing deadlines; therefore, the Department must correct overpayments and underpayments in a subsequent pay period.

Errors in overseas Civilian Pay accounts often occur due to payment of an entitlement that erroneously continued after the employee has returned to the United States. These improper payments often result from inaccurate personnel actions generated by human resources offices. Corrections subsequently are generated by human resource offices and transmitted to the civilian payroll system. These corrections result in pay and allowance re-computations therefore creating a collection action to offset the overpayment. The initial improper payments are discovered through agency reviews, bi-weekly exception reports, and employee or supervisor notification.

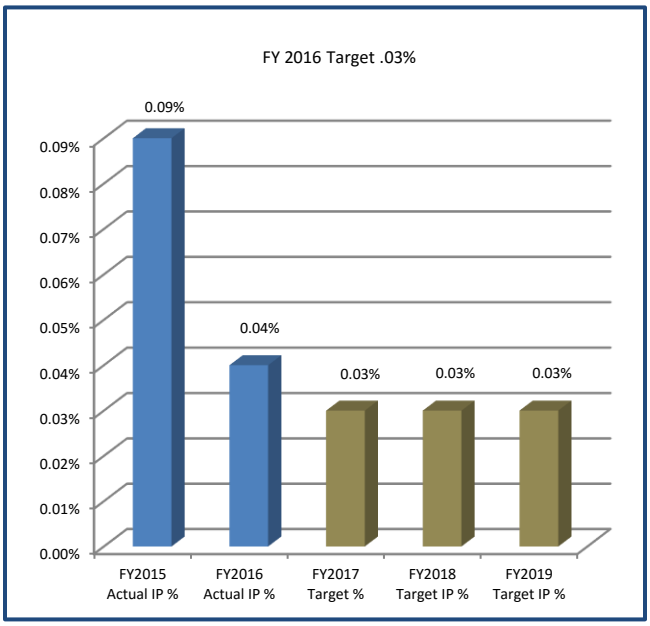
Commercial Pay

DFAS. The FY 2016 estimated improper payment amount is $110.82 million, with a 95 percent confidence interval, and an estimated 0.04 percent error rate. DFAS continued the current sampling methodology, stratified by invoice dollar amount, to conduct statistically valid reviews of invoices computed in the MOCAS contract payment system, the DFAS legacy commercial pay systems (IAPS, ONEPAY, CAPS), and the Army (GFEBS) and Defense Agency Component ERPs (DAI, EBS, DEAMS, and NERP). For NERP, DFAS reviews the invoices paid by DFAS.

Root Causes. The Commercial Pay improper payments result from administrative and documentation errors. Improper payments identified from quarterly random sample reviews include administrative errors, 100 percent, resulting from voucher examiner error, erroneous interest paid, and failure to provide special pay instructions.

Business Activity Monitoring (BAM) Tool. Using the BAM tool, DFAS identifies and prevents improper payments in a prepayment environment in the Department's five largest commercial payment systems, which includes MOCAS, CAPS-W, IAPS, One-Pay, and EBS accounting. These systems comprise approximately 87 percent of all DoD commercial payment dollars.

Figure 22: Improper Payment Rate - DFAS Commercial Pay



Since the implementation of BAM in August 2008, the tool has prevented a significant amount of improper payments. Continuous payment error analyses allow for the recurrent enhancement of BAM logic and improved disbursement accuracy.

This year, DFAS enhanced BAM criteria (integrity checks) to identify and prevent potential improper payments to improve the tool's performance. An example of the success of these enhancements is the strengthening of vendor payment integrity checks by utilizing more accurate data fields for comparisons.

DFAS identifies and monitors the root cause for all improper payments by researching supporting documentation and assigning an assessment (reason) code that identifies the type and cause of the improper payment. In addition, root causes of potential improper payments detected by BAM are reviewed and analyzed monthly. Root cause analysis is shared with the DFAS payment offices on a monthly basis and is used to identify areas for operational improvement. It is also used to implement refinements to BAM and develop new integrity checks.

USACE. USACE projected a 0.00 percent error rate for Commercial Pay for FY 2016.

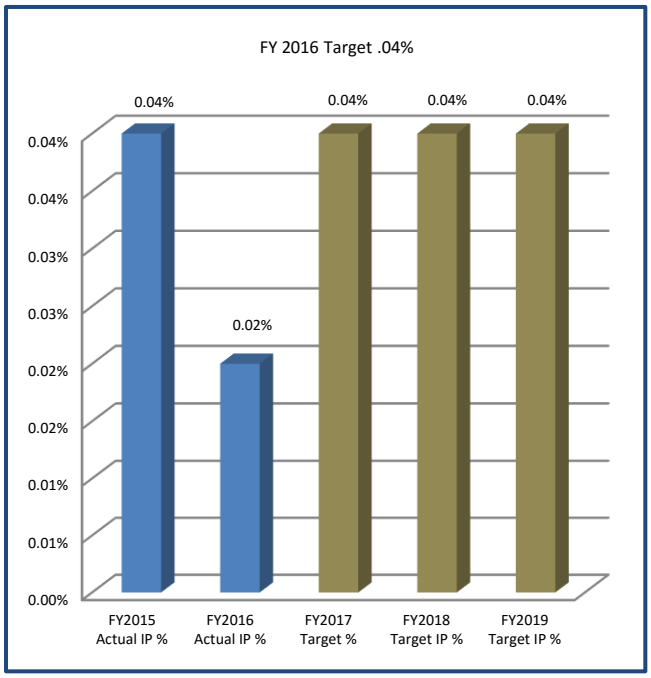
Navy. The Navy ERP projected a 0.00 percent error rate for Commercial Pay for FY 2016.

Military Retiree and Annuitant Benefit Payments. The Department projects a 0.02 percent error rate for the Military Retirement Program for FY 2016. Nearly 100 percent of the errors identified resulted from payments made by DFAS to deceased retirees or annuitants prior to DFAS receiving notification of their passing.

Root Causes. Eligibility for military retired pay ends on the retiree's date of death. Prompt reporting of a deceased retiree's death can help avoid possible financial hardship to the Service member's annuitant by expediting the correct calculation and processing of the monthly benefit. Family members or executors are required to return any overpayments of a deceased retiree's military retired pay.

Untimely notification of a retiree's or annuitant's death, by family members or other entities, often results in an initial, unavoidable overpayment to a deceased retiree. A review of overpayments to deceased retirees in FY 2016 disclosed that the Department recovered approximately 93 percent of overpayments within 60 days of initial notification of the retiree's or annuitant's death.

Figure 23: Improper Payment Rate - Military Retirement



Travel Pay

Department. The Department projected a 7.23 percent error rate for travel improper payments for FY 2016. This represents DTS trip records and WinIATS Temporary Duty (TDY) and Permanent Change of Station (PCS) vouchers for both civilians and military members, which are computed and disbursed by DFAS. In addition, the 7.23 percent error rate includes travel payments disbursed outside of DFAS by the Navy.

DFAS. DFAS reports the largest portion of DoD's travel payments, processed in DTS and WinIATS for the Department of the Army and select Defense Agencies. On a monthly basis, DFAS statistically samples DTS travel vouchers stratified by Military Service and the aggregate of the Defense Agency vouchers. In addition, DFAS also statistically samples monthly WinIATS travel vouchers, stratified by Army activity and type of payment, for both Temporary Duty Travel (TDY) and PCS. The DFAS improper payment rate for FY 2016 was 8.11 percent, a reduction from the FY 2015 DFAS improper payment rate of 8.80 percent. Comparatively on a system basis, the FY 2016 improper payment rate for the DTS was 8.43 percent. The FY 2016 improper payment rate for the WinIATS was 5.45 percent.

DTS Root Causes. The primary reason for DTS improper payments is voucher input errors by the traveler. In addition, approving officials' failure to identify error(s) prior to authorizing reimbursement contributed to improper payments from an internal control perspective. Moreover, the errors identified in the sample can be reported as administrative errors or errors that may result in an actual loss of funds to the government. The administrative errors include missing or invalid receipts (as defined in the Joint Travel Regulations (JTR)) or omission of required elements (i.e., dates and/or signatures).

- Administrative Errors represent over half of total errors (administrative and monetary).
- Receipts: Failure to attach receipts to the travel voucher, invalid or incorrect receipts, and illegible receipts.
- Signatures/Dates: Failure of the traveler and/or approving official to sign and/or date the DD Form 1351-2, Travel Voucher, prior to submission by the Non-DTS Entry Agent (NDEA) into DTS.
- Monetary errors that may result in an actual loss of funds.
- Statement of Non-availability (SNA): An SNA is required prior to payment of funds for members assigned to a war zone for separate lodging, meals and other expenses.
- Meals & Flat Rate Per Diem: Failure to properly pay flat rate per diem (partial per diem) once a member is TDY for 31 or more days.
- Lodging: The attached receipt for lodging does not reflect the same amount claimed on the travel voucher.
- All other monetary errors, not categorized above, include a combination of 28 additional categories.

WinIATS Root Causes. The primary reasons for WinIATS improper payments are voucher input errors by the traveler and/or the approving official's failure to identify the error(s) before reimbursement occurs. Error types include:

- Signatures/dates: Failure by the traveler, approving official or certifying official to sign and date the travel voucher or the voucher is approved prior to the end of the TDY;
- International Military Education & Training (IMET): IMET represents almost half of all overpayments identified in WinIATS and is caused by dating and submitting travel vouchers, by the student, prior to completion of training. IMET regulations were updated during December 2015 and as a result errors have been reduced. Overpayments attributed to IMET are non-collectable via a recovery process. Recovery is accomplished by the Department of State through subsequent year offsets and reductions to allocations;

- Unauthorized Individually Billed Account (IBA): Travelers are directed to use Centrally Billed Accounts (CBAs) vice IBAs to procure travel by the order writing authority. Procurement via an IBA is not authorized; and
- Meals and M&IE: Mispaid for reasons including wrong locality (per diem rate), wrong meal rate, paid while on leave, etc.

USACE. The Army Corps of Engineers continued working to reduce its Travel Pay error rate over the past 12 months (refer to Table 1). The USACE continues to emphasize and promote refresher training for all approving officials and travelers, which positively impacts the error rate. Also, the UFC performs a 100 percent audit of all airline credits issued against travelers' individually billed travel card accounts. This ensures that all airline credits, issued as a result of flight changes, are properly recouped.

Root Causes (see also Table 2). The primary reasons travel pay errors occur are:

- Errors generated by travelers when completing their travel vouchers; and
- Improper review of travel vouchers by Approving Officials (AO).

V. Corrective Actions

Military Health Benefits.

Corrective Actions. The DHA purchased-care contractors are monetarily incentivized or dis-incentivized, through payment accuracy performance standards, to reduce and/or eliminate improper payments. The fewer improper payments the contractors make, the less money is deducted from their reimbursements.

Additionally, details of the EIC compliance reviews are shared with the purchased-care contractors, DHA Program Offices, purchased-care contract Contracting Officers, and Contracting Officer Representatives to coordinate appropriate corrective action plans with the respective purchased-care contractor.

- Upon completion of an EIC compliance review, respective contractors review results, formulate an action plan to mitigate future findings and derive a process to avoid future improper payments.
- If warranted, contractor claims processing systems are modified to meet the Department's healthcare policy, reimbursement, or benefit requirements.
- If audit results show a potential error pattern for a certain type of claim, additional claims are pulled to conduct a focused study, and adjustment actions are taken as appropriate.

Each purchased-care contractor has its own business process for evaluating compliance review results, conducting root cause analyses to ensure the accuracy of future claims payment, and developing internal corrective action plans. If required, DHA Contracting Officers and

Contracting Officer Representatives issue contractor corrective action plans to resolve and track noncompliance with TRICARE healthcare policy/regulations and purchased-care contracts.

Military Pay

Corrective Actions. The Department institutes comprehensive training programs with standard desk procedures to ensure continuity of operation as new payroll clerks onboard. In addition, the Department, primarily through DFAS, advises the Military Services of the results of payment reviews and the associated root causes of the errors. DFAS provides the Military Service with monthly reports on the results of statistical reviews, including the reasons for and dollar value of errors and year-to-date trends, to enhance service training.

Civilian Pay

Corrective Actions. DFAS continues to advise Components of the results of payment reviews and the associated reasons for errors that result in improper payments to civilian employees. DFAS also advises Components on best business practices to prevent future improper payments and participates in various conferences to guide personnel on how to correctly submit information to prevent improper payments.

Commercial Pay

Corrective Actions. The Department continues to implement corrective actions to prevent, identify, and reduce overpayments. Corrective actions include:

- Ongoing training for pay technicians to increase their ability to compute and input claims accurately;
- Creation of a new database in MOCAS, Accounts Payable, that can provide reports highlighting data inaccuracies on the front end of the payment process;
- Continuing to work with Contracting Officers to simplify contract terms and eliminate the need for manual calculations;
- Initiating multiple special projects targeting specific problem areas to increase data accuracy and reduce payment errors; and
- Continuing electronic commerce improvement initiatives, such as the automation of third party payments, aimed at minimizing manual intervention and improving quality.

DFAS is working to add Procedures Guidance and Instruction (PGI) data to enhance detection capability within MOCAS. The PGI is a MOCAS system and Enterprise Solutions and Standards, Accounts Payable (ESS AP), Continuing Controls Maintenance initiative that created special payment instruction codes and data fields. These new data elements present an opportunity for new integrity checks to be created within the BAM tool for MOCAS.

Another initiative to reduce improper payments includes reaching out to the various sites to inform them of findings and results of reviews based on monthly ESS AP analysis of detected

improper payments. This site outreach is designed to reduce vendor billing errors caused by duplicate manual and electronic submission of invoices. In addition, the Department conducts manual reviews to ensure it meets all Certifying Officer Legislation requirements prior to certifying payment, such as ensuring proper documentation and correct payment amounts before disbursement.

Military Retiree and Annuitant Benefit Payments

Corrective Actions. The Department's control processes to prevent, identify, and reduce overpayments to deceased retirees and annuitants include:

- Validating existence of retiree and/or annuitant, if living outside the United States;
- Certifying, annually, the existence and entitlement for all annuitants:
    - Who are under 55 years of age;
    - Who receive hard copy checks in a foreign country; and
    - Who have a permanent disability (regardless of age);
- Conducting periodic, random certifications for retirees over a certain age; and
- Validating military retiree's existence if payments are returned and/or if a benefit account was suspended for several months due to bad check/correspondence address.

Early detection and data mining efforts, along with partnerships with other Federal and state entities, are used to detect improper payments. The Department takes a proactive approach to ensure the accuracy of Military Retiree payments by routinely comparing retired and annuitant payroll master file databases with the Social Security Administration's (SSA) Death Master File (DMF), and periodically comparing records with the Office of Personnel Management's deceased files, Department of Veterans Affairs' database, and with individual states with sizable retiree and annuitant populations (e.g., Texas, California, and Florida). Payments for military retirees identified as deceased are suspended pending validation of death or validation of continued eligibility. The Department's expanded definition of acceptable source documents for notice of death has allowed DFAS to initiate earlier reclamation actions, thereby enhancing faster recovery of overpaid funds. Refer to the Do Not Pay discussion, later in this section, for discussion on the Department's use of the Social Security DMF.

Travel Pay

DFAS.

DTS Corrective Actions. In early FY 2017 DFAS will launch a post-pay database consolidating its Travel Pay reviews and results. The database will allow DFAS to provide DoD leadership with timely, detailed information to assist in identifying root causes, recovery of funds, and other data at the service and activity level. The enhancement will provide information to use on the front-end of travel pay to reduce the improper payment rate. This will be an addition to the

error trend reports that DFAS provides to the DoD Components. Also, the Department continues its use of the DoD Travel Policy Compliance Tool, discussed in the Payment Recapture Audit Reporting section of this report.

WinIATS Corrective Actions. DFAS implemented steps to prevent improper payments, including:

- Conducting monthly meetings with post payment reviewers and Travel Pay operations personnel to discuss findings and preventative measures. DFAS has implemented a review forum to implement common policy between all parties engaged in computing, establishing policy, or conducting reviews.

USACE.

Corrective Actions. The USACE continues to educate travelers and travel AOs through required training, including refresher training for seasoned travelers and AOs. Additionally, all AOs are required to complete fiscal law training every year to maintain their certification. When improper payments are identified, the UFC notifies the parties involved to determine the circumstances surrounding the error and to assist them in identifying business process improvements to prevent future recurrences. These areas are also covered thoroughly in refresher training.

Navy.

Corrective Actions. In FY 2016, the Department of the Navy continued to work with DFAS and its two services (US Navy and Marine Corps) to validate root causes and implement corrective actions, including improvements to reports, classification of improper payments, updated sampling plans, and improved training.

VI. Internal Controls over Payments

Table 6 summarizes DoD risk assessments (1-4) within each internal control standard.

Table 6. Status of Internal Controls

Internal Control Standards	DHA*	Navy ERP Com Pay	Navy Com Bill Pay Naples	WINIATS	USACE Com Payments	USACE Travel Payments
Control Environment	3	4	4	3	4	4
Risk Assessment	3	4	4	2	4	4
Control Activities	3	4	4	2	4	4
Information and Communication	3	4	4	2	4	4
Monitoring	3	4	4	3	4	4

NOTE: *DHA consists of North, South, West, TDEFIC, TOP, TPharm and ADDP.

Definitions:

1=Controls are not in place to prevent improper payments.
2=Minimal controls are in place to prevent improper payments.

3=Controls are in place to prevent improper payments, but there is room for improvement.
4=Sufficient controls are in place to prevent improper payments.

DFAS. The Managers' Internal Control Program and the DFAS FY 2016 Statement of Assurance provided reasonable assurance to management that controls for operations, financial reporting, and financial systems were/are established and operating effectively.

DHA. DHA has payment accuracy performance standards requiring contractors to meet TRICARE policy or contract performance standards or be subject to financial penalty. The current baseline for contractor performance standard is 1.75 percent. However, DHA Program Offices have developed more stringent contract performance requirements lowering the requirement to less than 1 percent.

DHA monitors contractor performance by conducting EIC compliance reviews. In addition, DHA has numerous prepayment (i.e., claims auditing software, TRICARE documentation policies, duplicate claim check) and post payment controls (i.e., EIC audits, DCAA contract audits, recovery activities, Medicare cost report and internal contractor post payment audits) built into the military health benefits contract requirements and contractor's claims processing systems to minimize improper payments.

Navy. During FY 2016 Navy performed a comprehensive review of its system of internal controls over improper payments. Improvement areas for FY 2017 include, updates to guidance, governance, risk assessments, sampling plans, "Tone at the Top" guidance, program management, user entity controls, and accountability through reporting.

USACE. USACE internal process controls are built into CEFMS and are an integral part of the overall business processes. Process controls include, but are not limited to: decentralization of support activities, certification and separation of duties requirements for disbursement of funds; documentation requirements for invoices (i.e., receiving reports); and disbursement limitations with respect to obligations (i.e., disbursement amounts cannot exceed obligation amounts).

VII. Accountability

The Under Secretary of Defense (Comptroller)/Chief Financial Officer is the Accountable Official for the Department and is responsible for ensuring that, to the greatest extent possible, all DoD disbursements are accurate.

Certifying Officer Legislation, *10 U.S.C. 2773a,* holds Certifying and Disbursing Officers accountable for government funds. In accordance with this law, pecuniary liability attaches automatically when there is a fiscal irregularity (i.e., (1) a physical loss of cash, vouchers, negotiable instruments, or supporting documents, or (2) an improper payment). This is further captured in the *DoD FMR, Volume 5, Chapter 3*, entitled, "Certifying Officers, Accountable Officials, and Review Officials." The Department's efforts to recover overpayments from a recipient must be undertaken in accordance with the debt collection procedures outlined in the *DoD FMR, Volume 16*, entitled, "Debt Management".

The DoD FMR contains other policies that specifically address Improper Payments *(DoD FMR Volume 4, Chapter 14*) and Recovery Auditing *(DoD FMR Volume 10, Chapter 22*). Beginning in Quarter 3, FY 2013, all reporting DoD Components were required to begin downloading their improper payment reports to the DFAS ePortal, as the Office of the Deputy Chief Financial Officer's Accounting & Finance Policy Directorate was designated as the Executive Agent to manage this information and its associated reporting requirements. This centralized electronic system allows the reporting Components to access improper payment information without regard to the time zone in which they are located. More importantly, it allows management to ensure all Components' submissions are timely and accurate.

Because DoD Travel currently has the highest error rate among all DoD-reported programs, the focus for the Department is to identify and reduce travel improper payments and enhance the recovery efforts for overpayments.

VIII. Agency Information Systems and Other Infrastructure

The Department has much of the information and infrastructure needed to reduce improper payments. The Department uses the BAM tool and the Do Not Pay portal to identify potential improper payments prior to disbursement.

The Department's ongoing migration from a legacy system environment to new ERP systems presents a number of challenges and opportunities to prevent and detect improper payments. This migration also can enhance the Department's ability to improve its debt collection and recovery

auditing abilities. The Department is addressing these areas both from a payment integrity as well as audit readiness perspective.

DHA. The DHA has much of the information and infrastructure needed to reduce improper payments. Purchased-care contractors utilize claims adjudication systems to determine the appropriate reimbursement methodology based on information included in the claims such as type of service, provider record, and claim form type. In addition, the Department analyzes data from the TRICARE Encounter Data Set (TEDS), representing payments as reported by purchased-care contractors. The TEDS contain various edits to verify patient and provider eligibility, benefit calculations, and reimbursement methodologies determined by DHA.

Further, the DHA has developed the TRICARE Duplicate Claims System (DCS). This tool facilitates the identification of duplicate claim payments, the initiation and tracking of recoupments, and the removal of duplicate records from the TEDS database. DHA purchased care contractors are contractually required to use the DCS and resolve duplicate payments.

IX. Statutory and Regulatory Barriers

The primary barriers in preventing improper payments in Military Pay are the statutory entitlements and regulatory monthly pay schedule. For DHA collections, there are contractual requirements that allow up to 270 days, instead of the standard delinquency deadline of 120 days, to be transferred to the Treasury under the Debt Collection Improvement Act of 1996.

X. Payment Recapture Audit Reporting

Table 7 shows improper payment recaptures.

Table 7. Improper Payment Recaptures with and without Audit Programs

Overpayments Recaptured outside of Payment Recapture Audits ($ in millions)			
Program or Activity	**Amount Identified**	**Total Amount Extrapolated (estimated throughout Total Outlays)**	**Amount Recaptured (Refunds throughout FY 2015) [4]**
Military Pay [1]	$183.66		$148.13
Civilian Pay [1]	$55.83		$55.83
Military Retirement [2]	$8.81		$8.28
DoD Travel Pay [3]	$2.30		$0.57
DFAS Commercial Pay	$185.50		$153.90
USACE	$5.00		$5.00
DHA [4]	$2.11	$121.60	$346.87

Note 1: Military Pay and Civilian Pay include In-Service Collections for recovery amounts. Military Pay also includes Out-of-Service Debts. Both In-Service Collections and Out-of-Service Debts continue to be collected beyond the AFR period.
Note 2: The amounts identified and recovered are based on 100% review of Deceased Retired and Deceased Annuitant accounts.
Note 3: The amounts identified and recaptured are based on the amounts identified in the statistical reviews. Overpayments for Foreign Students (IMET) are not subject to recovery and are not included.
Note 4: DHA "Amount Recaptured" represents dollars paid back to DHA throughout FY 2015. These refunds include overpayments identified in FY 2015 audits as well as refunds occurring in the course of routine claim adjustments (for claims initially paid in FY 2015 and other fiscal years). These refunds also include claims for TPharm claims that were not conducted (see footnotes for Table 1).

DoD Travel Policy Compliance Tool. In December 2012, the Department established the DoD Travel Policy Compliance Program, mandated by the National Defense Authorization Act for FY 2012. Managed by the Defense Travel Management Office, the program was established to ensure travel claims do not exceed reasonable or actual expenses as well as to minimize inaccurate, unauthorized, overstated, inflated, or duplicate travel claims. The DoD Travel Policy Compliance Tool, an automated application, reviews DTS travel vouchers in near real time and identifies potential improper payments. If a potential improper payment is identified, travelers and their AOs are notified via e-mail to either submit a corrected claim or explain why the claim is correct. Service administrators can run reports to review all identified errors and track corrections.

The DoD Travel Policy Compliance Tool not only assists in recouping funds, but it also improves post-payment audits, educates travelers and administrators on travel policy, and identifies opportunities for greater controls in the future. As of September 30, 2014, all DoD Components using DTS are actively using the Compliance Tool, and all DTS vouchers are being examined using 12 areas of inquiry.

As of September 26, 2016 (cumulative since December 26, 2012):

- $16,433,501[13] in errors were identified;
- $4,031,769 in payment errors were corrected without any funds due back to the Government;
- $2,745,834 in errors were corrected and are awaiting collection; and
- $7,242,129 in errors were corrected and the funds have been recovered.

In addition to examining DTS vouchers, the Compliance Tool has expanded to include additional data sources, such as Government Travel Charge Card (GTCC) data, and is now comparing amounts claimed on vouchers with amounts charged on the GTCC to identify potential overpayments. As new data sources become available, they may be used to identify additional errors.

Use of the Compliance Tool provides a mechanism to greatly facilitate DoD's collections and improve the recovery rate for Travel Pay overpayments. In addition, funds recovered from prior years can be re-allocated for use in current year appropriations, in accordance with Public Law 111-204, IPERA.

DFAS. The Department continues to use its internal staff and procedures to identify and recover overpayments. The DFAS recovery percentages remain close to the 85th percentile, as required by OMB. The use of the BAM tool on the front-end of commercial payment transactions continues to provide a successful means of preventing improper payments and thereby reducing the need to pursue overpayment recoveries.

In early FY 2017, DFAS will launch a post-pay database consolidating its Travel Pay reviews and results. A key feature of this database will be the inclusion of additional fields to provide more detailed front-end data. The database will enable DFAS to provide DoD leadership with increasingly actionable data to reduce improper payments. It will function in addition to the error trend reports that DFAS provides to the DoD Components. Also, the Department will continue to use the DoD Travel Policy Compliance Tool.

In compliance with IPERIA, as well as the *Debt Collection Improvement Act of 1996*, the Department uses a number of other methods to prevent, identify, and collect improper payments. For example, DFAS has implemented a Centralized Offset Program to look across the Components for opportunities to offset debts within the first 90 days of delinquency. Once this deadline passes, DFAS transfers the debts to the Treasury Department, no longer waiting until day 120 as allowed by statute, to utilize all debt collection tools available earlier in the debt lifecycle to increase the likelihood of collecting the debt. During FY 2016, the Centralized Offset Program requested and confirmed 901 offsets totaling approximately $7.00 million.

[13] DoD Travel Policy Compliance Program numbers provided are cumulative from the beginning of the program (December 26, 2012)

USACE. The UFC uses a data mining tool as part of its post payment/payment recapture program. This tool searches for potential errors, such as duplicate, missing, or irregular invoices, as well as specific types of recurring payments. There are ten scenarios built into the data mining tool, which searches 100 percent of all USACE commercial payments. The use of a data-mining tool complements the prepayment system edits built into CEFMS. Payment safeguards include a requirement to match a receiving report with an invoice and thereby prevent use of duplicate invoice numbers for the same obligation.

DHA. The DHA uses a number of different mechanisms to prevent, identify, and collect improper payments, to include claims auditing by an EIC, contractor utilization of the DHA DCS, and periodic independent reviews of private-sector payments. All overpayment recoveries are returned to the MHBs program.

Contract payments comprise a large volume of transactions with high-dollar values; therefore, DHA is vigilant to ensure payment accuracy. In addition to the post-payment reviews, the DHA also utilizes various internal manual and automated prepayment initiatives to prevent overpayments and underpayments.

XI. Disposition of Funds Recaptured Reporting

The Department has no reportable data for "Disposition of Funds Recaptured through Payment Recapture Audits".

XII. Aging of Outstanding Overpayments Reporting

The Department has no reportable data for "Aging of Outstanding Overpayments in the Payment Recapture Audits".

XIII. Additional Information

The Department is committed to full compliance with the requirements of IPERIA and the Federal Improper Payments Coordination Act of 2015. As part of the Department's audibility efforts, each disbursing Component is diligently reviewing and reporting all payments subject to IPERIA and the Federal Improper Payments Coordination Act of 2015, as well as examining processes for identifying the complete universe of disbursements.

Moreover, the Department continues to explore measures to improve its front-end internal controls to prevent improper payments, and strengthen post payment review teams to recover identified improper payments. Also, the Department is actively implementing recommendations from the following reports:

- DoD IG 2016 report, "DoD Actions Were Not Adequate to Reduce Improper Travel Payments" (Report No. DODIG-2016-060); and
- GAO 2013 report, "Significant Improvements Needed in Efforts to Address Improper Payment Requirements" (Report No. GAO-13-227).

Accordingly, the Chief Financial Officer issued a policy memorandum, "Preventing Travel Pay Improper Payments and Enforcing Recovery" on October 7, 2016. The memorandum included a Travel Pay Improper Payments Remediation Plan. Also, the Department continues to adopt best practices related to statistical sampling and improved system controls, procedures, and guidance. Presently, the Department is implementing dollar-stratified sampling for Travel Pay, Military Pay, and Civilian Pay to obtain a sample population that best represents the entire population for those programs.

XIV. Agency Reduction of Improper Payments with the Do Not Pay Initiative

Table 8 summarizes the Department's successes attributed to the Do Not Pay Initiative.

Table 8. Results of the Do Not Pay Initiative in Preventing Improper Payments

	Number (#) of payments reviewed for possible improper payments	Dollars ($) of payments reviewed for possible improper payments (in millions)	Number (#) of payments stopped	Dollars ($) of payments stopped	Number (#) of potential improper payments reviewed and determined accurate	Dollars ($) of potential improper payments reviewed and determined accurate (in millions)
DFAS NTDO reviews with the IPERIA specified databases	6,620,895	$644,638.11	0	$0.00	84,709	$5,227.11
DFAS TDO reviews with the IPERIA specified databases*	0	$0.00	0	$0.00	0	$0.00
DHA Reviews with the IPERIA specified databases	438	$1,754.14	0	$0.00	438	$1,754.14
USACE Reviews with the IPERIA specified databases	304,481	$82,044.00	0	$0.00	360	$29,819.94

*Non Treasury Disbursing Office (NTDO) Data is based on invoice and invoice amount vs. payment.

The Do Not Pay (DNP) Initiative (detailed reporting in Table 7), as currently implemented, is programmed to verify that vendors are in fact authorized to receive payments from DoD. Improper payments may still occur at some later point due to reasons that DNP cannot detect.

DFAS. DFAS sends a Commercial Pay weekly batch file, made up of invoices in a non-pay status, to the DNP database and receives results the next day. DFAS then researches these results to determine if the payment is proper based on established business rules. To date, DFAS has not identified any potential improper payments using the DNP list.

DFAS continues to conduct comparisons against all the DNP databases with the exception of the debt check, which is a duplication of the Treasury Offset Program, and the Credit Alert System, which does not apply to Commercial Payments. 98% of the false positives received, are based on the death master database results along with name match results from the rest of the DNP databases. The other 2 percent are deemed not to be improper payments due to established business rules related to performance in accordance with the contract.

USACE. The USACE matches its payment files daily in the DNP Portal to prevent any improper payments.

DHA. Individual Payments. The DHA processes relatively few (5-20) case recoupment refunds each month for small dollar amounts ($5 – $20,000). The Single Online Search service is utilized before any payment is distributed to verify (1) a business or individual has not been placed on the List of Excluded Individuals/Entities, and (2) an individual has not died. Any matches will be referred to the DHA Office of General Counsel.

Vendor, Contract Payments. The DHA processes approximately 260 routine payments per month for 19 unique contractor payees. The Single Online Search service is utilized once a month, before payments are distributed, to verify that each DHA contractor payee has not been placed on the Excluded Parties List System or the List of Excluded Individuals/Entities. Any matches are validated with the Treasury Offset Program ensuring the contractor does not have the same Employer Identification Number as a person's Social Security Number. The contractor is responsible for resolving these matching issues due to proprietary reasons. If the contractor is on the list, the finding is referred to the assigned Contracting Officer. DHA processed approximately 438 payments totaling $1,754,135,258.78 with no matches on the Do-Not-Pay system for FY 2016.

The risk for payments to a subcontractor or individual via the contractor, however, lies outside of DHA control. DHA contractors are not required to utilize the Do-Not-Pay database, and there is no current mechanism in place to require the contractors to use the Do-Not-Pay databases at the prepayment phase to comply with the Federal Improper Payments Coordination Act of 2015.

Navy ERP. Navy ERP transactions are included in the DFAS Do Not Pay Figures.

Military Retiree and Annuitant Benefit Payments – File Matching with the Death Master File outside DNP

Prior to implementation of the Do Not Pay initiative, the DMDC had a computer matching agreement with SSA to use its DMF to identify potential accounts that need to be suspended or cancelled as a result of a retiree's or annuitant's passing. As part of the end-of-month processing, DFAS produces two files (one for retirees, one for annuitants) that are sent to DMDC to match or

conduct comparisons against the monthly DMF file. The results are compiled and forwarded to DFAS.

DFAS then runs its match process to suspend pay accounts (but not cancel) and to notify next of kin that this action was based on information received from SSA. This correspondence contains instructions on how to close out the account or reactivate if the death was mistakenly reported by SSA; however, this is rare.

The vast majority of these monthly benefits are paid via Electronic Funds Transfer (EFT). The disbursement system suspends payment to prevent additional benefits from being improperly paid. Any EFT payment that was mistakenly disbursed is automatically reclaimed from the bank account after the official notification of death is processed. The normal recovery rate is approximately 95 percent within 60 days of the official death confirmation.

An Airman from Dover Air Force Base is basket-lifted by a Coast Guard H-65 Dolphin helicopter during water survival training Aug. 6, 2015, Bowers Beach, Del. Airmen with the 512th Airlift Wing and 436th Airlift Wing performed water survival training focusing on treading water, raft survival, and the basket lift helicopter evacuation.

U.S. Air Force photo by Tech. Sgt. Nathan Rivard

FREEZE AND REDUCE THE FOOTPRINT

DoD supports the principles of OMB's plan, National Strategy for the Efficient Use of Real Property (2015-2020), Reducing the Federal Portfolio through Improved Space Utilization, Consolidation and Disposal, by demonstrating a continual reduction in the DoD infrastructure footprint. Since the inception of the government wide plans to freeze and then reduce the footprint of the federal real property inventory, DoD has been the leader among Federal agencies by contributing over 50 percent of the total federal footprint reduction. As of the FY 2015 Federal Real Property Profile submission, DoD has disposed another 4,238,768 square feet in office and warehouse footprint.

Since most of DoD's infrastructure is not likely candidates for consolidation or reuse by other Federal Agencies, much of the DoD reduction must be in the form of demolition. Since demolition incurs an initial cost to produce eventual operating savings, frequent budget cuts have had a negative impact on the funding of much needed demolition. But DoD continues to aggressively pursue plans for supporting the Reduce the Footprint initiative within the current budgetary constraints. The DoD Reduce the Footprint implementation plan for the period FY 2017-2021 projects an additional reduction of another 35,928,100 square feet of real property.

Since the original FY 2012 Baseline was established for Freeze the Footprint, there was a realization that some assets types were not correctly identified in the correct categories for counting the new Reduce the Footprint policy. A decision was made to use the time between FY 2012 data and the FY 2015 Federal Real Property Profile (FRPP) submission to properly align the assets into correct categories. The FY15 FRPP would then establish a new baseline for Reduce the Footprint.

Table 9: Freeze the Footprint Baseline Comparison

	FY 2012 Baseline	FY 2015 Adjusted Baseline	Change (FY 2012 – FY2015)
Square Footage (SF in millions)	313.5	339.2	25.7

Table 10: Annual Operating Costs

	FY 2012 Calculated Cost	FY 2015 Calculated Cost	Change (FY 2012 - FY2015)
Annual Operating Costs ($ in millions)	13,510. 5	14,665.1	1,154.7

CIVIL MONETARY PENALTY ADJUSTMENT FOR INFLATION

On November 2, 2015, the President signed into law the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (the 2015 Act), which further amended the Federal Civil Penalties Inflation Adjustment Act of 1990 (the Inflation Adjustment Act). The 2015 Act, Public Law 114-74, requires DoD to annually adjust applicable civil monetary penalties for inflation to improve the effectiveness and retain the deterrent effect of such penalties. The implementation of this rule will deter violations of law, encourage corrective action(s) of existing violations, and prevent waste, fraud, and abuse within the Department.

Name of Penalty	Authority (Statute)	Year of Previous Adjustment	Year of Current Adjustment	Current Penalty Level ($ Amount)
Unauthorized Activities Directed at or Possession of Sunken Military Craft	National Defense Authorization Act for FY 2005, 10 U.S.C 113, note	2004	2016	$124,588.00
Unlawful Provision of Health Care	10 U.S.C. 1094(c)(1)	1996	2016	$10,940.00
Wrongful Disclosure—Medical Records: First Offense Subsequent Offense	10 U.S.C. 1102(k)	1996	2016	 $6,469.00 $43,126.00
Violation of the Pentagon Reservation Operation and Parking of Motor Vehicles Rules and Regulations	10 U.S.C. 2674(c)(2)	1990	2016	$1,782.00
Violation Involving False Claim	31 U.S.C. 3802(a)(1)	1996	2016	$10,781.00
Violation Involving False Statement	31 U.S.C. 3802(a)(2)	1996	2016	$10,781.00

SCHEDULE OF SPENDING

Department of Defense Combined Schedule of Spending Agency Wide		*Dollars in Millions*
For the Years Ended September 30, 2016 and 2015	**2016**	**2015**
What Money is Available to Spend?		
Total Resources	**$ 1,101,472.0**	**$ 1,067,434.3**
Less: Amount Available but Not Agreed to be Spent	(115,136.1)	(109,503.1)
Less: Amount Not Available to be Spent	(40,500.1)	(39,998.1)
Total Amounts Agreed to be Spent	**$ 945,835.8**	**$ 917,933.1**
How was the Money Spent/Issued?		
Civil Work		
Personnel Compensation and Benefits	$ 3,842.5	$ 2,364.6
Contractual Services and Supplies	9,001.4	9,977.1
Acquisitions of Assets	4,191.0	4,074.3
Grants and Fixed Charges	13.2	7.8
Other	1,370.9	1,273.1
Total Civil Works	**18,419.0**	**$ 17,696.9**
Military Retirement		
Personnel Compensation and Benefits	$ 9,721.9	$ 9,507.8
Contractual Services and Supplies	0.0	0.0
Acquisitions of Assets	0.0	0.0
Grants and Fixed Charges	57,242.3	56,829.0
Other		
Total Military Retirement	**$ 66,964.2**	**$ 66,336.8**
Military Personnel		
Personnel Compensation and Benefits	$ 120,195.8	$ 120,770.4
Contractual Services and Supplies	7,488.3	7,241.5
Acquisitions of Assets	20.6	0.6
Grants and Fixed Charges	380.8	288.1
Other	16,550.6	16,699.8
Total Military Personnel	**$ 144,636.1**	**$ 145,000.4**
Operation, Readiness & Support		
Personnel Compensation and Benefits	$ 164,176.2	$ 147,748.2
Contractual Services and Supplies	279,952.7	313,317.6
Acquisitions of Assets	23,265.3	18,499.7
Grants and Fixed Charges	2,401.6	2,055.2
Other	28,991.0	12,705.8
Total Operations, Readiness & Support	**$ 498,786.8**	**$ 494,326.5**

Department of Defense Combined Schedule of Spending Agency Wide		*Dollars in Millions*
For the Years Ended September 30, 2016 and 2015	**2016**	**2015**
Procurement		
Personnel Compensation and Benefits	$ 97.2	$ (3.9)
Contractual Services and Supplies	24,485.5	23,696.3
Acquisitions of Assets	96,815.8	80,330.0
Grants and Fixed Charges	233.5	142.9
Other	435.1	3,265.5
Total Procurement	**$ 122,067.1**	**$ 107,430.8**
Research, Development, Test & Evaluation		
Personnel Compensation and Benefits	$ 4,872.4	$ 4,555.4
Contractual Services and Supplies	66,730.3	57,995.4
Acquisitions of Assets	9,002.0	5,616.8
Grants and Fixed Charges	1,654.8	1,687.4
Other	(442.3)	4,434.8
Total Research, Development, Test & Evaluation	**$ 81,817.2**	**$ 74,289.8**
Family Housing and Military Construction		
Personnel Compensation and Benefits	$ 743.9	$ 848.4
Contractual Services and Supplies	2,587.3	2,015.9
Acquisitions of Assets	7,294.5	7,228.4
Grants and Fixed Charges	82.2	24.6
Other	2,437.5	2,734.6
Total Family Housing and Military Construction	**$ 13,145.4**	**$ 12,851.9**
Total Amounts Agreed to be Spent	**$ 945,835.8**	**$ 917,933.1**

The Combined Schedule of Spending presents an overview of the funding received by the Department and how it was spent (i.e., obligated) during the reporting period. The Schedule of Spending presents total budgetary resources and fiscal year-to-date total obligations for the reporting entity. The budgetary information in the Schedule of Spending is presented on a combined basis and not a consolidated basis in order to remain consistent with the information reported on the Report on Budget Execution and Budgetary Resources (SF-133) and statement of budgetary resources.

DOD INSPECTOR GENERAL'S SUMMARY OF MANAGEMENT AND PERFORMANCE CHALLENGES FOR FY 2016

Each year, DoD IG prepares a statement summarizing the most serious management and performance challenges facing the Department and provides a brief assessment of the Department's progress in addressing these challenges.

For FY 2016, the DoD IG identified challenges in the following ten categories:

- Countering Global Strategic Challenges
- Countering the Terrorist Threat
- Enabling Effective Acquisition and Contract Management
- Increasing Cyber Security and Cyber Capabilities
- Improving Financial Management
- Protecting Key Defense Infrastructure
- Developing Full Spectrum Total Force Capabilities
- Building and Maintaining Force Readiness
- Ensuring Ethical Conduct
- Promoting Continuity and Effective Transition Management

The DoD IG's memorandum and report on "Top Management and Performance Challenges Facing the Department of Defense" follows, reprinted in its entirety as received.

U.S. Marines with Combined Anti-Armored Team, 1st Battalion, 1st Marine Regiment, taking part in Exercise Koolendong 16 and are part of the Marine Rotational Force-Darwin, stop to scan for targets while training in maneuvering through a wooded area in a convoy operation at Bradshaw Field Training Area, Northern Territory, Australia Aug. 8, 2016.

U.S. Marine Corps photo by Sgt. Sarah Anderson

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

October 5, 2016

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: Top Management and Performance Challenges Facing the Department of Defense

Public Law (PL) 106-531, the "Reports Consolidation Act of 2000," requires that Inspectors General prepare an annual statement that summarizes what they consider to be the "most serious management and performance challenges facing the agency." PL 106-531 further states that the "agency head may comment on the inspector general's statement, but may not modify the statement." By statute, this statement is required to be included in the Department's Agency Financial Report.

Attached is the Department of Defense Office of Inspector General's statement regarding the top management and performance challenges facing DoD. The challenges outlined in this statement were identified based on our oversight work, research, and judgment; as well as our consideration of oversight work done by other components within the DoD and the Government Accountability Office.

In this statement, we summarize each challenge, outline steps the DoD has taken to address it, and discuss ongoing future oversight work related to the challenge. This year's list identifies the top ten challenges as:

- Countering Global Strategic Challenges
- Countering the Terrorist Threat
- Enabling Effective Acquisition and Contract Management
- Increasing Cyber Security and Cyber Capabilities
- Improving Financial Management
- Protecting Key Defense Infrastructure
- Developing Full Spectrum Total Force Capabilities
- Building and Maintaining Force Readiness
- Ensuring Ethical Conduct
- Promoting Continuity and Effective Transition Management

The OIG looks forward to working with the DoD to continually improve the DoD's efforts to address these important challenges.

Glenn A. Fine
Acting Inspector General

1 – Countering Global Strategic Challenges

Global Threats from China, Russia, Iran, and North Korea

Interagency Cooperation

Evolving global threats are a top challenge for the DoD. Secretary of Defense Carter has identified the five most significant global strategic challenges to U.S. interests as Russia, China, North Korea, Iran, and terrorism. In a speech at a Center for New American Security conference on March 17, 2016, The Secretary stated that these threats require new ways of planning, budgeting, and operating. He noted that the DoD must have the capability to staff, equip, and deploy personnel and equipment to combat multiple challenges throughout the world.

Maintaining a level of preparedness to address multiple global threats poses major management challenges for the DoD.

Global Threats

As the Secretary stated in his testimony to the Senate Armed Services Committee on September 22, 2016, "We don't have the luxury of choosing between these challenges, which is why American soldiers, sailors, airmen, and Marines are working with partners from our worldwide coalition in more ways and with more power every day."

With regard to the challenge from China, the 2017 Defense Posture Statement reported that the specific U.S. objective in Asia and the Pacific is "maintaining freedom of navigation and overflight, full and unimpeded lawful commerce, and that disputes are resolved peacefully." To accomplish this, he said, "the United States will continue to fly, sail, and operate wherever international law allows."

However, in recent years, China has undertaken aggressive and expansionist reclamation activities in the South China Sea and East China Sea. By creating artificial islands in maritime territory claimed by multiple neighboring countries, China has increased regional tensions and presented a significant challenge to U.S. interests in the region. Additionally, China has been building and improving its military capabilities, such as nuclear weapons, ballistic and cruise missiles, counter-space and offensive cyber capabilities, electronic warfare systems, a stronger, more lethal surface and submarine warfare capability, and a more sophisticated air force.

At a June 2016 conference, the Secretary stated, "Although we have disagreements with China, especially over its destabilizing behavior in the South China Sea, we're committed to working with them and to persuade them to avoid self-isolation. That is one reason why we'll continue to pursue a stronger, bilateral military-to-military relationship with our colleagues in China." The Secretary

also emphasized the importance of maintaining trilateral and multilateral country relationships in the Asia-Pacific region in support of U.S. strategic interests.

Similarly, the Chief of Naval Operations at the same conference noted that the United States has many strong bilateral relationships in the Pacific but that increasing trilateral and multilateral collaboration is key to maintaining regional stability.

In addition to security challenges in the Pacific region posed by China, North Korea and its pursuit of nuclear weapons and ballistic missile technologies, and its role in their proliferation, presents a growing strategic threat. North Korea directly threatens its neighbors, South Korea and Japan, with which the United States has security treaty commitments. Moreover, North Korean leaders regularly assert that the United States is its principal enemy.

According to the Secretary in the 2016 Defense Posture Statement, the DoD is working to develop a comprehensive set of alliance capabilities to counter the growing North Korean ballistic missile threat. In that regard, the United States and South Korea jointly announced consultations concerning the feasibility of deploying a Terminal High-Altitude Area Defense system to the Korean peninsula. The United States currently maintains a significant ground, air, and sea force based in South Korea and Japan to deter North Korean aggression. Any aggression by North Korea against the security of South Korea or Japan could require a U.S. response and appropriate action by DoD and its U.S. Forces Korea command.

According to the Secretary's 2017 Defense Posture statement, Russia's increasingly aggressive posture in Europe poses major challenges. The posture statement notes that "Russia has in recent years appeared intent to erode the principled international order that has served us, our friends and allies, the international community, and also Russia itself so well for so long." Russia has violated the sovereignty of the Ukraine, Moldova, and Georgia, and it actively seeks to intimidate its Baltic neighbors. In addition to seizing the Crimea, sovereign territory of the Ukraine, Russia has deployed a significant military force to the eastern Ukraine and continues to threaten to destabilize the rest of the country. Its tactics range from the use of media manipulation, support for right-wing political parties, cyber weapons that can disrupt critical infrastructure, and hostile intervention by Russian military aircraft flown dangerously close to ships and aircraft from the U.S. and North Atlantic Treaty Organization (NATO).

Russia is making a significant investment in building its military capabilities. It has modernized its forces to develop, for example, an asymmetric, unconventional warfare capability and new weapons systems. It has also enhanced training of its military personnel and units and strengthened their discipline.

Russia's advanced military systems also seek to threaten U.S. advantages in certain areas we have traditionally dominated, such as the capability to disrupt battlefield communications and the use of precision artillery. This has prompted the United States and NATO allies to reinforce their internal security capacity to deter or respond to Russian aggression. In addition, the United States and NATO are committed to building the military capabilities of the Baltic Republics, as well as those of Poland and Romania, through training, advising, and equipping their forces.

According to White House officials, through the European Reassurance Initiative, the DoD is seeking to build the resilience and capability of our allies and partners and to enable a quicker and more robust response in support of NATO's common defense. This initiative increases the presence of U.S. and NATO forces in Europe through stepped-up unit rotations and continued deferral of some planned force reductions. In addition, U.S. and NATO forces have deployed units to Baltic countries and Romania, Poland, and Bulgaria. U.S. and NATO forces are also conducting training and joint exercises with these partner countries' security forces. The total U.S. investment in the European Reassurance Initiative has quadrupled over the past year, from $789 million to $3.4 billion proposed for FY 2017.

Iran also poses increased global security threats. Its continued sponsorship of regional terrorist groups and its nuclear ambitions require the DoD to maintain an adequate deterrent capability and ensure that the United States can immediately respond if Iran commits acts of aggression. For example, as the Secretary of Defense stated in in his testimony on March 17, 2016, "We must still deter Iranian aggression and counter Iran's malign influence against our friends and allies in the region, especially Israel, to whom we maintain an unwavering and unbreakable commitment." According to the 2017 DoD Defense Posture Statement, Iran supports the Assad regime in Syria, backs Hezbollah in Syria and Lebanon, and is contributing to disorder in Yemen, while still directing hostility and violence to the United States' closest ally in the region, Israel.

Finally, the threat from terrorism and the other strategic threats discussed above underscore the DoD's need to maintain an adequate deterrent capability. Given the simultaneous nature of the evolving threats, the need for continual upgrades in weapons systems and force readiness is a challenge particularly under the resource constraints imposed by the DoD budget. These and other related management challenges are discussed throughout this document. We address in the next section of this document the need for interagency cooperation in addressing these five evolving global threats.

Interagency Cooperation

The DoD must work with other key elements of the U.S. Government to confront evolving strategic challenges. Interagency cooperation and unity of effort are fundamental to countering global threats successfully. For example, in September 2014, President Obama announced a

comprehensive strategy to degrade and ultimately destroy the Islamic State in Iraq and the Levant (ISIL), setting out nine strategic lines of effort to combat its terrorist activities. These nine lines of effort cross agency lines and include active military operations throughout the world, financial and investigative activities among coalition partners, cutting off terrorists' resources, countering ISIL's messaging, and law enforcement activities that protect the homeland. Each line of effort is assigned a designated lead agency or agencies for coordinating and implementing activities, including the Departments of Defense, State, Treasury, and Homeland Security, as well as the U.S. Agency for International Development, the Director of National Intelligence, and the National Counterterrorism Task Force.

Interagency cooperation in the oversight of these activities is critical. For example, section 8L of the Inspector General Act of 1978, as amended, mandates that a Lead Inspector General (IG) develop and carry out a joint strategic plan to conduct comprehensive oversight of all aspects of contingency operations. The DoD IG has been appointed the Lead IG for the two current contingency operations for Operation Inherent Resolve (OIR), the effort to degrade and destroy ISIL, and Operation Freedom's Sentinel (OFS), the effort to provide support to Afghanistan to help build and sustain an enduring security capability. The Inspectors General for the U.S. Department of State and U.S. Agency for International Development are key partners in fulfilling the oversight requirements associated with the Lead IG activities. The objective of Lead IG oversight is to ensure adequate oversight of any contingency operation through either joint or individual audits, inspections, and investigations. The Lead IG and supporting IGs continue to identify and make recommendations to correct inefficiencies and ineffectiveness in programs throughout their respective agencies. These cooperative efforts are ongoing and collectively reported on a quarterly basis.

In short, the DoD, individually and through interagency efforts, faces a difficult management challenge to effectively combat evolving and growing strategic threats throughout the world.

2 – Countering the Terrorist Threat

Developing Partner Security Forces
Insider Threat

As noted in the previous section, countering terrorist threats remains a top challenge and a critical national security priority. For example, on September 27, 2016, the Director of the National Counterterrorism Center testified before Congress stating, "Having passed the 15-year mark since 9/11, the array of terrorist actors around the globe is broader, wider, and deeper than it has been at any time since that day." He added, "The threat landscape is less predictable and, while the scale of the capabilities currently demonstrated by most of these violent extremist actors does not rise to the level that core al-Qaida had on 9/11, it is fair to say that we face more threats originating in more places and involving more individuals than we have at any time in the past 15 years."

In its strategic guidance document, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," the DoD identified countering "non-state threats" as part of a complex set of challenges in the global security environment. The document further stated that the DoD will continue working with allies and partners to establish control over ungoverned territories and directly strike the most dangerous groups and individuals when necessary.

With regard to threat to DoD forces and insider threats, in a recent statement to the Senate Armed Services Committee, Secretary Carter discussed the importance of countering the terrorist threat to DoD personnel and facilities. He stated that the DoD is working to ensure "force protection for our troops and the DoD facilities where they work and reside—both on base, and the thousands of off-base installations we operate. Last summer's tragedy in Chattanooga Tennessee, underscored how ISIL seeks to target U.S. troops and DoD civilians, which is why we're putting in place stronger physical security systems, including stronger entry controls, better alarm systems, reinforced doors, additional ways to safely exit our facilities, and more."

In addition to threats posed by foreign entities, the DoD also seeks to counter internal threats by developing insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat to national security. According to the National Counterintelligence and Security Center, "the most damaging U.S. counterintelligence failures, over the past century, were perpetrated by a trusted insider with ulterior motives."

Building Partner Capacity

According to its strategic guidance document, the DoD views building partnership capacity as an essential strategy in helping to respond to terrorism as well as sharing the costs and responsibilities of this ongoing challenge. Accordingly, the DoD's strategy addressed regional military challenges by partnering with and helping to develop the military capabilities of allied nations. A major DoD program for working with foreign militaries is the Defense Institution Building program, which is managed by the Defense Security Cooperation Agency. The Defense Institution Building Program's aim is to establish responsible defense governance to help partner nations build effective, transparent, and accountable defense institutions.

In Iraq, the United States and its coalition partners are engaged in OIR, the mission to degrade and destroy ISIL. According to the 2017 Defense Posture Statement, the U.S. strategy includes providing military support to coalition partners and making significant investments in training, advising, assisting, and equipping the Iraqi Security Forces (including Kurdish and Sunni Popular Mobilization forces), and in enabling moderate Syrian anti-ISIL forces.

This is a difficult mission with no easy solutions, particularly in Syria. The train, advise, assist, and equip program is essential to building the capacity of Iraqi security forces. Iraqi Sunni tribal

forces and vetted Syrian opposition forces were key to OIR progress in 2016. Iraqi Sunni tribal forces supported the liberation of Sunni-dominated Falluja, and the Syrian fighters succeeded in liberating Manbij and closing the Turkish border to ISIL.

Several DoD OIG oversight reviews examined aspects of the fight against ISIL. For example, a September 2015 DoD OIG assessment evaluated U.S and Coalition efforts to train, advise, and assist the Iraqi Army to initiate and sustain combat operations to defeat ISIL. The report made recommendations that the U.S and Coalition authorities update operational and program plans, communications and quality assurance processes, and improve the mentorship of Ministry of Defense personnel.

Ongoing DoD OIG oversight efforts are assessing U.S and Coalition efforts to train, advise, assist, and equip the Kurdish Security Forces, the Iraqi Counterterrorism Service, and Iraqi Special Operations Forces. Future oversight will examine U.S and Coalition efforts to build the capacity of the Iraq Federal Police, DoD's analysis of information contained in social media in support of OIR, and whether DoD and the U.S. Department of State are effectively planning and coordinating stabilization efforts in Iraq and Syria.

In Afghanistan, the United States is conducting operations through OFS against terrorist groups in the region. The United States is also supporting the NATO-led Resolute Support Mission to develop the institutional capacity of Afghanistan's Ministries of Defense and Interior to support and sustain the Afghan National Defense and Security Forces (ANDSF). The United States faces ongoing challenges in its efforts to develop a self-sustaining ANDSF. Moreover, the pace of progress in building Afghan national institutions and effective leadership within those institutions is slow and may be insufficient to achieve broad U.S. objectives in a reasonable time frame.

Prior DoD OIG oversight in Afghanistan identified key challenges in these efforts, such as inadequate capacity of the Ministries of Defense and Interior to lead and sustain the ANDSF; poor asset accountability and sustainment of vehicles and equipment; and insufficient logistic sustainment capability within the Afghan National Police. Shortcomings in building adequate systems to sustain growing Afghan security forces is a recurrent theme in DoD OIG oversight work and underlies many of the ANDSF capability gaps that have been identified. For example, the DoD OIG has found that mechanisms to provide supplies, equipment, maintenance, and personnel to Afghan army and police forces remain immature and unreliable.

Other oversight organizations, such as the Special Inspector General for Afghanistan Reconstruction (SIGAR) have identified challenges with building partner capacity. For example, an April 2016 report, coauthored by SIGAR and the U.S. Institute of Peace, identified lessons learned in the international efforts to rebuild Afghanistan. The report cited a number of challenges, including the need to address conflicting goals held by the various parties involved in Afghanistan.

The report noted that warfighting goals are focused on immediate effects on the battlefield while developmental goals focused on sustainable achievements resulting from multiyear efforts. The report found that many nations were unclear as to what they were trying to achieve in Afghanistan or how to prioritize their warfighting versus development goals.

The report also found that the Coalition lacked shared, well-defined donor objectives and goals. Finally, with regard to improving chances for success in Afghanistan, the report noted that the success of development efforts hinged on donors' knowledge of the local areas and their ability to gain the buy-in of Afghans living there. However, donors' ability to tailor their efforts to local needs was often undermined by inappropriate measures of progress, inability to move around the country, and frequent rotation of personnel.

Future DoD OIG oversight will examine the Afghan Ministry of Interior's development of its internal controls capability; the Afghan government's controls over U.S. direct funding assistance; and U.S and Coalition efforts to train, advise, and assist the Afghan Air Force. DoD OIG intelligence assessments will also focus on U.S. counterterrorism capabilities and effectiveness in support of OIR and OFS.

In an April 2016 review, the GAO cited building partner capacity as a central focus of the U.S. counterterrorism strategy, as underscored by the allocation of $675 million for Global Train and Equip program activities in fiscal year 2015. The allocation was a sharp increase compared to the $275 million annual average in the preceding 6 years. The GAO concluded that although DoD had established an interagency process to develop and select security assistance project proposals, the DoD did not require documentation of receiving units' capacity to absorb the assistance offered or fully document consideration of other key elements in planning fiscal year 2015 projects. According to the GAO, fully documenting the basis of project approval decisions could enhance transparency, provide additional assurance that resources are efficiently allocated, and help ensure the long-term benefits of projects and careful use of scarce U.S. and partner nation resources.

Insider Threat

It is also important to recognize that threats to the United States, its citizens, and its military can come from insider threats, not only foreign governments and terrorist groups. Perhaps the most compelling recent example of an insider threat that has caused great harm to U.S. intelligence gathering capabilities is the case of Edward Snowden. He is the former National Security Agency contractor employee who remains a fugitive due to his admitted theft and release of classified National Security Agency information. In 2014, President Obama stated that Snowden's leaks of classified information revealed "methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come."

Insiders can further can commit terrorist acts or cause harm to U.S. personnel or organizations because they have an awareness of their organization's vulnerabilities or exploitable security measures. Insiders can engage in terrorist activities through compromising sensitive information or through the use or threat of violence.

For example, in November 2009, an Army officer shot and killed 13 people and wounded 32 others on base at Fort Hood, Texas. That officer had exchanged e-mails with an al Qaeda figure asking whether individuals that attack fellow soldiers were considered martyrs. In September 2013, a Navy contractor killed 12 civilian employees and contractors and wounded 4 others at the Washington Navy Yard, D.C., in an act of workplace violence.

DoD's reviews of each incident resulted in numerous recommendations associated with personnel policy, installation security, force protection, casualty response, and support to DoD healthcare providers. A July 2015 GAO report concluded that the majority of policy and guidance related to DoD's key force protection had been updated, but some guidance did not yet reflect insider threat considerations. The GAO further found that while selected installations have taken actions to protect against insider threats, the DoD has not consistently shared this information, and the DoD was still in the process of implementing recommendations from the Fort Hood and Washington Navy Yard reviews.

In May 2016, the DoD required contractors, for the first time, to establish and implement their own insider threat program to detect, deter, and mitigate insider threats. The revised National Industrial Security Program Operating Manual requires contractors to have a written program plan in place to begin implementing revised insider threat requirements no later than November 30, 2016.

In 2014, the DoD also created the Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System. The system's purpose is to analyze, monitor, and audit insider threat information for insider threat detection and mitigation within DoD concerning DoD and U.S. Government installations, facilities, personnel, missions, or resources. The system supports insider threat programs, enables the identification of systemic insider threat issues and challenges, provides a basis for the development and recommendation of solutions to mitigate potential insider threats, and assists in identifying best practices amongst other Federal Government insider threat programs. Future DoD OIG oversight will assess whether the DoD Insider Threat Management and Analysis Center has adequate controls over the collection, analysis, and dissemination of insider threat and workplace violence information.

To address insider threat concerns involving the security of military housing, the DoD OIG reviewed access controls for general public tenants leasing housing on military installations and found that DoD officials did not ensure that tenants were properly screened before granting

unescorted access to installations. Additionally, access badges were issued with expiration dates that exceeded tenants' lease terms. As a result, the DoD assumed an unnecessary safety and security risk to military personnel, their dependents, civilians, and assets.

In sum, while the DoD recognizes the challenges posed by insider threats, they remain a vulnerability and require continued focus from the DoD.

3 – Enabling Effective Acquisition and Contract Management

Linking Requirements to Strategic Military Plans Contract Management and Oversight
Illegal Technology Transfer

Acquisition and contract management have been high-risk areas for the DoD for many years. Although Congress and the DoD have long sought to improve the acquisition of major weapon systems, many DoD programs are still falling short of cost, schedule, and performance expectations. This can result in unanticipated cost overruns, program development spanning decades, and, in some cases, a reduction in the capability ultimately delivered to the warfighter.

In addition to acquisition challenges, the DoD obligates more than $300 billion annually on contracts for goods and services, including support for military installations, information technology, consulting services, and commercial items. The DoD must also reengineer its processes to evaluate contracts for spare parts pricing and manage its contracts for weapons system support.

Furthermore, the DoD must continually focus on preventing the illegal transfer of operational and defense technologies.

Acquisition Challenges

The scope and size of acquisition programs for DoD weapon systems is enormous. As of April 2016, the DoD portfolio of defense acquisition programs totaled 1,375 programs. In the FY 2017 Presidential Budget, the DoD requested $183.9 billion to fund those acquisition programs. Over the past year, the number of programs in the DoD portfolio of major defense acquisitions increased from 78 to 79, while its total planned investment in these programs decreased from $1.45 trillion to $1.44 trillion.

In recent years, the DoD has taken steps to improve the acquisition of major weapon systems, such as implementation of DoD's Better Buying Power initiatives. In 2010, the DoD launched these initiatives to strengthen the DoD's buying power; improve industry productivity; and provide an affordable, value-added military capability to the warfighter. The Better Buying Power initiatives provide a set of fundamental acquisition principles to achieve greater efficiencies through

affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition. The initiatives are also designed to incentivize productivity and innovation in industry and Government, and improve the processes for the acquisition of services.

Despite this initiative and these positive steps, acquisition programs continue to exceed the cost and schedule defined in the program's strategy documents. DoD OIG audits have found program managers contribute to acquisition challenges by approving concurrent development and testing of software and hardware during production that expose programs to undue risks of additional design changes and costly retrofits. For example, the DoD OIG evaluated the Navy's efforts to prepare and manage the Ship-to-Shore Connector ship acquisition program for initial production. The DoD OIG found that program officials' plan to conduct concurrent developmental testing and production may require the Navy to make substantial and costly modifications resulting from design and integration deficiencies found during production. The DoD OIG found in other audits that some programs are proceeding into production before manufacturing processes are fully established, which causes cost and schedule delays.

According to the DoD, the promotion of competition is a central tenet in acquisition reform and the single best way to motivate contractors to provide the best value. However, a GAO assessment of weapons programs found inconsistent use of acquisition strategies that include competition. Of 43 programs that GAO assessed as a part of its 2016 selected weapon programs assessment, 21 programs conducted or planned to conduct competitive prototyping before development start and 26 had acquisition strategies that included some measure to encourage competition after development start. In addition, 13 programs reported pursuing measures to promote competition both before and after the start of system development. GAO found that those programs experienced less development cost growth than those that promoted competition in only one phase of acquisition. GAO also reported its prior work has shown that competitive prototyping can help programs reduce technical risk, refine requirements, and validate designs and cost estimates prior to making major commitments of resources. Programs that do not take this step may miss an opportunity to lower costs and reduce risk.

Overall, DoD OIG audits have determined that the DoD has made progress in acquisition program management, but the DoD continues to experience programmatic problems, such as cost overruns and schedule delays in acquisition programs. For example, the DoD OIG has continued to identify acquisition challenges in which:

- program personnel inappropriately requested waivers and deferrals from operational test requirements;
- program personnel certified that programs were ready for initial operational test and evaluation when programs were not;
- program personnel did not adequately document the acquisition process to define, validate, fund, and execute requirements; and

- programs did not meet system performance requirements.

Additionally, the DoD OIG continues to identify other challenges in the acquisition process. For example, contracting personnel did not:

- always determine fair and reasonable prices for spare parts,
- acquire excess spare parts inventory, and
- adequately manage contracts for weapons system support.

The DoD OIG made specific recommendations to address these challenges, and the Services have made progress in implementing them. For example, the DoD OIG evaluated the Navy's management of waivers and deferrals from operational test requirements for nine major weapon systems. The DoD OIG review of waiver requests at the Naval Air Systems Command found that Navy program managers and system sponsors did not fully implement Navy policies for requesting waivers and deferrals before certifying if the programs were ready for Initial Operational Test and Evaluation to support the final production decision. As a result, six of nine programs reviewed completed Initial Operational Test and Evaluation with unresolved deficiencies that negatively impacted the warfighter's primary missions. The Navy took immediate actions by issuing interim guidance to address the gaps in the testing and identification of deficiencies caused by program offices unchecked use of the waiver and deferral process. Additionally, the Vice Chairman of the Joint Chiefs of Staff updated the Manual for the Operation of the Joint Capabilities Integration and Development System to include a requirement that program managers notify Joint Requirement Oversight Council when a program is not meeting its primary mission requirement. In another review, the DoD OIG we found that the Army plans to spend $2.52 billion over 20 years to procure and maintain 501,289 carbine rifles that its own analysis shows could be delayed for another 10 years with no negative impact to the warfighter. The Army agreed with the DoD OIG recommendation to eliminate funding for the program.

In another example, the DoD OIG determined that the Army should specifically define the capability requirements to increase the likelihood that the Integrated Air and Missile Defense Battle Command System, valued at approximately $6.4 billion, would provide useful and supportable capabilities that could be effectively developed, tested, and produced at an affordable cost. The Under Secretary of Defense for Acquisition, Technology, and Logistics agreed to postpone the initial production decision until the project manager completes testing that shows the Army system will meet the planned requirements. The Commander, Army Fires Center of Excellence, agreed to fully define system capability requirements for the planned second increment of the system.

Moreover, the acquisition of weapon systems that meet warfighter requirements is critical to enabling the United States to implement its strategic military plans. From 2001 through 2014, test results for 123 weapons systems developed as major defense acquisition programs showed that over 40 percent of weapons systems managed as major defense acquisition programs could not fully

meet mission requirements at the time of initial deployment. The discovery of programs not meeting performance requirements at this late phase of the development process results in further unforeseen delays.

Software development is one major factor that affects the ability of weapon systems to meet mission requirements. In a March 2016 assessment of selected DoD weapons programs, the GAO found that of 55 programs assessed, 40 reported software development as a high-risk area. According to the GAO report, the three most common reasons for high risk in software development were the challenge of completing the software development needed to conduct developmental testing; underestimating the difficulty of the originally planned software effort; and hardware design changes that necessitate additional software development.

Despite DoD's efforts to reduce waste, accelerate schedules, and control costs, new weapon systems are regularly fielded later than originally planned, which results in increased expenses in DoD's acquisition programs. Part of the problem is that weapons manufacturers are incentivized to submit optimistic cost and schedule estimates to be awarded major contracts. Service officials may agree with these projections to protect their acquisition budgets. Weapons system program managers, caught in the middle, want to avoid disruption stemming from comparing optimistic cost estimates with unrealistic performance requirements after their programs have started.

The DoD OIG typically audits programs that are 15 to 18 months from a major acquisition milestone decision. Since FY 2013, the DoD OIG has identified about $31 billion in acquisition program quantities that were not validated or properly approved. Additionally, the DoD OIG have determined the capability requirements have not been adequately defined and tested and that test community recommendations or deficiencies have not been adequately addressed and, in some cases, ignored. Acquisition reform has not alleviated DoD OIG findings that programs continue to exceed cost and schedule baselines and have not adequately defined performance metrics.

In FY 2017, the DoD OIG plans to perform additional audits on the acquisition process, including acquisitions on programs such as the Navy Expeditionary Fast Transport program, Marine Corps Amphibious Assault Vehicle, Navy Mine Countermeasures Mission Package, and Army and Marine Corps Joint Light Tactical Vehicle.

Contract management and oversight

The DoD spends approximately $300 billion each year on contracts for services and supplies. It faces challenges with contracting for sustainment contracts, procuring domestically produced items, contracting with small business, oversight of contracting officer's representatives (CORs), and completing assessment reports on contractor performance.

DoD OIG oversight of DoD's contracting continues to identify challenges with sustainment contract costs. For example, the DoD OIG identified an Air Force contract in which, over a 4-year period, $1 billion was spent without achieving its acquisition objective of increasing aircraft availability while decreasing sustainment costs. Also, in another instance, the DoD OIG found that DoD invested in a modernization program to update its aircraft, reduce operating costs, and extend the service life for decades without fully validating almost $60 million in sustainment costs.

The DoD also struggles to comply with the Berry Amendment and the Buy American Act. The Berry Amendment promotes the purchase of goods produced in the United States by directing how the DoD can use funds to purchase items such as fabrics, food, and hand tools. The Buy American Act of 1933 requires, with certain exceptions, that only articles, materials, and supplies that have been mined, produced, or manufactured in the United States are used to fulfill Federal procurement and construction contracts. Overall, the DoD OIG has found that the Services did not consistently comply with the Berry Amendment and the Buy American Act.

Contracting personnel were not always familiar with legal and DoD requirements to procure items produced in the United States. Additionally, contracting personnel issued contracts that did not include the appropriate contract clauses to implement the Berry Amendment and Buy American Act. Service personnel had limited assurance that the purchased items complied with the Buy American Act, and suppliers may have provided items that were not produced in the United States. Contracting personnel also may have violated the Anti-deficiency Act when they used appropriated funds to purchase non-domestically produced items when domestically produced items were available.

The Federal Acquisition Regulation requires the Federal Government to provide maximum practicable opportunities in its acquisitions to small business. Small businesses must also have the maximum practicable opportunity to participate as subcontractors in the contracts awarded by any executive agency that is consistent with efficient contract performance. The DoD's contracting with small businesses has improved. For example, in FY 2015, the DoD exceeded its goal for awarding prime contracts to small businesses.

The DoD OIG's work has identified that the DoD is at risk for contractors passing inflated costs to the DoD but not savings. Furthermore, subcontract evaluations present additional challenges. Major subcontractors often represent 50 percent or more of total cost on major defense acquisition programs. Prime contractor access to subcontractor cost or pricing data, including historical actual costs, may be limited, resulting in the DoD overpaying for those subcontractor costs. As of August 2016, the DoD OIG identified that the DoD spent at least $194 million more than fair and reasonable prices for commercial and noncommercial spare parts. Additionally, we estimate that the DoD could spend an additional $402.5 million more than fair and reasonable prices for spare

parts based on expected future use. This is a systemic challenge that has not vastly improved, although the DoD OIG has issued more than 30 reports on spare-part pricing in the last 18 years.

The DoD also continues to struggle with providing effective contract oversight. Specifically, DoD OIG audits determined that contracting officers did not always appoint CORs, CORs were not always adequately trained, contracting officials did not always develop adequate quality assurance surveillance plans or were missing them altogether, and CORs did not always maintain supporting documentation. Some contracting officers did not define responsibilities for CORs, or assigned multiple contracts to one COR who may not have had sufficient time to perform all oversight responsibilities. The CORs did not use the oversight procedures established in the quality assurance surveillance plan to monitor contractor performance.

Without effective oversight by CORs, the DoD will not have sufficient information to assure goods and services received are consistent with contract quality requirements and performed in a timely manner.

The DoD OIG has also identified significant problems with past performance reporting across the DoD. The Federal Acquisition Regulations require that contractor performance information be collected and used in source selection evaluations. Source selection officials should rely on clear and timely evaluations of contractor performance to make informed business decisions when awarding Government contracts and orders. This information is critical to ensuring that the Federal Government only does business with companies that provide quality products and services in support of DoD missions. DoD OIG audits have found that DoD officials have not evaluated contractor performance in accordance with guidance.

Illegal Technology Transfer

Technological superiority is critical to U.S. military strategy. The DoD spends billions each year to develop and acquire sophisticated technologies that provide an advantage for the warfighter during combat or other missions. Many of these technologies are also sold or transferred to other countries to promote U.S. economic, foreign policy, and national security interests. These technologies can also be acquired through foreign investment in U.S. companies that develop or manufacture them. However, sensitive DoD technology is also a target for unauthorized transfer, such as theft, espionage, reverse engineering, and illegal export.

The DoD continues to face the challenge of preventing the illegal transfer of these sensitive technologies. To avoid illegal technology transfer, U.S. technology must be transferred in accordance with U.S. export control laws. The U.S. Export Control Act regulates the transfer of U.S. technology, including arms and defense technology.

Each year, the Defense Security Service publishes a report of its findings on foreign attempts to collect sensitive or classified information and technology. In the FY 2015 report, the Defense Security Service reported a continued increase in reported foreign collection attempts to obtain sensitive or classified information and technology. These collection attempts targeted all aspects of DoD technologies, including electronics; command, control, communication, and computers; aeronautic systems; and marine systems.

The Defense Security Service report identified the most common methods of operation, including academic solicitation, suspicious network activity, and attempted acquisition of technology through commercial, government, and government-affiliated organizations. The report stated that the threat faced by illegal transfer of DoD technology "shows no sign of waning, and securing our cutting-edge technology remains key to maintaining our military and economic advantage."

The DoD has published agency-wide policies and worked to strengthen programs to identify and protect technologies critical to U.S. interests. The Defense Security Service administers the National Industrial Security Program for DoD and 30 other Federal agencies. Recognizing that U.S. industries develop and produce the majority of U.S. defense technology, the National Industrial Security Program ensures DoD contractors properly safeguard classified information and information associated with critical technologies. To remain a facility that is cleared by the National Industrial Security Program, DoD contractors must meet specific requirements to ensure they are safeguarding critical technologies in their possession while negotiating bids, contracts, programs or performing research and development efforts. DoD policy requires DoD organizations and contractors to report unlawful attempts to access or illegally transfer critical technologies to the appropriate counterintelligence or law enforcement agency.

As the criminal investigative arm of the DoD OIG, the Defense Criminal Investigative Service (DCIS) conducts counter-proliferation investigations that pertain to the illegal transfer of sensitive DoD technologies. As of September 30, 2016, the DCIS had 198 open counter- proliferation cases that represent approximately 12 percent of its active investigations. In FY 2016, the DCIS counter-proliferation investigations resulted in 12 criminal charges, 11 convictions, and over $20 million in recoveries for the Government.

The DCIS routinely works with counterpart Federal law enforcement agencies and de-conflict investigative activity through the Department of Homeland Security's Export Enforcement Coordination Center. The following examples highlight a few of recent DCIS investigations.

Three Chinese Nationals affiliated with the Chinese company HK Potential were arrested in Connecticut and convicted for a scheme to steal and illegally export sophisticated U.S. military semiconductors. These semiconductors were designed for ballistic missile and satellite applications. To conceal the theft, the perpetrators provided counterfeit semiconductors to replace

the original semiconductors. One defendant has been sentenced to 15 months confinement and was ordered to forfeit $63,000. The other two defendants are awaiting sentencing. In a separate case, a California woman was convicted and sentenced to 50 months in prison for conspiring to export fighter jet engines, an unmanned aerial vehicle and related technical data to China in violation of the Arms Export Control Act. In another example, a Chinese National was arrested for illegally attempting to export high-grade carbon fiber to China. The individual allegedly expressed a willingness to pay a premium to avoid U.S. export laws. The carbon fiber, which has many aerospace and defense applications, is strictly controlled.

In short, the DoD has initiated several initiatives to improve its acquisition and contract management processes. However, more needs to be done to reduce the high risks within acquisition and contract management. In addition, steps need to be taken to ensure arms and defense technology must be transferred in accordance with U.S. export control laws.

4 – Increasing Cyber Security and Cyber Capabilities

Offensive and Defense Operations
Technology Platforms and Infrastructure

Since 2013, the Director of National Intelligence has identified cyber threats as the top strategic global threat facing the United States. In testimony to Congress in 2013 and 2014, the Director cited a wide range of potential adversaries who attempt to disrupt or manipulate U.S. activities, relying on digital technology or the Internet. The GAO also identifies cybersecurity of Federal information systems and networks as a high-risk area because all sectors of the Government-energy, transportation systems, communications, financial services, and defense of the homeland-are dependent on information systems and electronic data to perform operations and to process, maintain, and report essential information.

The DoD has become increasingly reliant on cyberspace to enable its military, intelligence, and business operations to perform the full spectrum of military operations without disruption, and cyber threats and exploitable vulnerabilities have grown substantially. The Secretary of Defense recognized the need to increase the DoD's cybersecurity efforts and has requested $6.7 billion in FY 2017 to support the DoD's cybersecurity efforts,

To guide DoD's cyber activities and operations, in 2011 the Secretary of Defense signed the initial "DoD Strategy for Operating in Cyberspace." This document also established the Cyber Mission Force, and, in 2012, the DoD began to build the Cyber Mission Force of approximately 6,200 military, civilian, and contractor support personnel to perform critical DoD cyber missions. The Cyber Mission Force performs defensive cyberspace operations, defends the United States and its interests against cyberattacks, and supports combatant commands in integrating cyberspace effects into command plans.

In April 2015, the Secretary of Defense issued a new DoD Cyber Strategy to build upon the initial concepts and set prioritized goals and objectives through 2020. This strategy defines three separate, but interdependent DoD cyber missions:

- defend DoD Information Networks, systems, and information;
- defend, in coordination with the Department of Homeland Security and other Federal agencies, the U.S. homeland and U.S. national interests against cyberattacks; and
- support combatant command operational and contingency planning.

In addition to the Cyber Mission Force buildup, the DoD has invested about $20 billion since 2012, earmarked for cybersecurity enhancements and technology acquisitions to improve its ability to protect DoD and U.S. interests from cyberattacks.

The Commander, U.S. Cyber Command, who is responsible for leading DoD offensive cyberspace operations, stated that the DoD has made progress in developing strategies and goals to combat cyber threats. However, the DoD continues to face significant challenges in protecting and securing its networks, systems, and infrastructure from cyber threats and in increasing its overall cyber capabilities. Cyberspace threats to the DoD continue to increase at an alarming rate. In April 2016, the Commander reported that cyberspace operations by a range of state and non-state actors have intensified against the DoD. The Commander cited individual criminal acts as the most significant number of attacks but noted that nation states, such as Russia, China, Iran, and North Korea, still represent the gravest threats to national security because they have the skills, resources, and patience to sustain sophisticated campaigns to penetrate and compromise DoD's networks. The Commander also stated that cyberattacks against the power grid, communications networks, and vital U.S. services could significantly affect command and control of DoD operations and, more broadly, the basic business functions of the United States.

Among other significant cyberattacks, North Korea conducted a cyberattack against Sony Pictures Entertainment, and the Chinese conducted a cyberattack against the Office of Personnel Management. Both cyberattacks affected security and had significant economic impacts. More recently, well-publicized cyberattacks have breached systems used by the Democratic National Committee, the Democratic Congressional Campaign Committee, and the World Anti-Doping Agency.

Defending DoD Information Technology Networks

The DoD must defend its many information technology networks, both unclassified and classified, from compromise. This is a significant challenge. The DoD Information Network is a globally interconnected, end-to-end set of information capabilities that collects, processes, stores, disseminates, and manages critical information. It includes owned and leased communications and computing systems and services, software, data, and security and other associated services.

The network seeks to design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, and confidentiality, as well as user authentication and nonrepudiation.

To improve its ability to defend the DoD Information Network, the DoD established the Joint Force Headquarters–DoD Information Network in January 2015 to lead and coordinate command and control decisions and tactical operations affecting the defense of DoD's systems, networks, and data. The Commander, Joint Force Headquarters–DoD Information Network, also coordinates with the Commander, U.S. Cyber Command.

The Commander, U.S. Cyber Command, also serves as the Director of the National Security Agency. The Secretary, Congress, and President are considering separating these commands. The GAO is currently assessing, among other things, the advantages and disadvantages of the Commander, U.S. Cyber Command, serving as the Director of the National Security Agency and how the DoD measures performance for this relationship in response to a proposed congressional mandate.

To assess the DoD's efforts to protect its information networks, the DoD OIG issued a report in 2013 on maintaining authorization accreditation for select DoD information systems. The report concluded that 2 of the 10 information systems reviewed operated on the DoD Information Network for as long as 14 months without proper security controls to continue their authorization agreements. The DoD OIG recommended that the Air Force take appropriate action to shut down network access or accept the risk of operating without approved security controls for all systems with expired authorities to operate.

The DoD OIG also conducted audits related to the protection of physical and logical access to the Secret Internet Protocol Router Network. The audits found consistent and systemic weaknesses that affected the security of the classified network. The DoD OIG recommended specific physical security improvements and other cybersecurity-related actions to limit access points, account for all circuits, and manage general and privileged account access. Although not completed, the Navy and Air Force have begun corrective actions to address specific and systemic weaknesses identified in these OIG audits.

Developing and Using Cyber Capabilities and Infrastructure

The DoD also faces challenges in developing or acquiring unique cyber capabilities to conduct defensive and offensive operations. In September 2015 testimony, the Deputy Secretary of Defense and the Commander, U.S. Cyber Command, stated that the DoD continues to develop a broad range of cyberspace capabilities and a separate infrastructure to respond to or conduct cyberspace attacks. In November 2015, however, the DoD OIG issued a classified report concluding that the Military

Services were independently developing cyber platforms and cyber capabilities, which could result in redundant capabilities that do not align with the mission needs of the Cyber Mission Force. Among other actions, the DoD OIG recommended developing a unified strategic plan to address capability development to meet both Service-specific and joint mission requirements. Although not completed, U.S. Cyber Command and the Military Services have begun to address joint capability development needs of the Cyber Mission Force.

The DoD is now building a unified platform to integrate disparate cyber platforms and capabilities. However, the unified platform will not be operational for several years. To ensure that the Cyber Mission Force and the Services are able to meet joint and Service-specific operational requirements, the DoD needs to unify capability development and accelerate research and development of cyber capabilities, including basic and applied research to develop cyber technologies that can be used in a wide range of operational environments.

Additionally, the DoD is in the process of implementing the Joint Information Environment, an initiative announced in August 2010 by the Secretary of Defense to consolidate information technology infrastructure to achieve savings in acquisition, sustainment, and manpower costs and improve the DoD's ability to defend its networks against growing cyber threats. This is designed, in part, to reduce the DoD Information Network attack surface by establishing a single security architecture, optimizing identity and access management, and migrating to cloud computing. However, since 2014, the DoD OIG and the GAO have issued reports on the DoD's challenges in implementing Joint Information Environment initiatives.

The DoD has been actively engaged with the National Institute of Standards and Technology to improve the understanding of cloud computing across the Federal Government and has implemented enhancements to the DoD's Select and Native Programming Data Input System for Information Technology to more accurately account for cloud budgets and to collect information on DoD cloud contracts.

However, in recent audit reports, the DoD OIG concluded that the DoD did not have an effective cloud computing implementation strategy or process to collect data and measure the effectiveness and efficiency of the DoD cloud initiative. The DoD OIG recommended that the DoD develop an implementation plan that described required tasks, resources, and milestones for transitioning to cloud services and establishing a repository for collecting cloud-related information.

The GAO also issued a report in July 2016 that concluded the DoD's almost $1 billion investment in the Joint Information Environment by yearend FY 2016 has yet to result in fully defining the scope and cost of the program. The GAO recommended defining the scope and expected cost of the Joint Information Environment and fully identifying the composition of the cyber workforce needed to operate within the program. In response to the report, the DoD stated

that it was in the process of completing documentation to address new Joint Information Environment program and cost assessments.

Planning and Conducting Defensive and Offensive Operations

Defensive and offensive cyberspace operations, whether conducted individually or simultaneously, are important for defending the U.S. homeland and national interests and supporting operational and contingency operations. In accordance with the October 16, 2012 Presidential Policy Directive-20, "U.S. Cyber Operations Policy," the DoD can conduct offensive and defensive cyberspace operations. For example, as part of OIR, the DoD is conducting offensive cyberspace operations to counter cyber threats and limit disruptive and destructive cyber capabilities used by ISIL and to disrupt and interrupt its ability to operate, communicate, and command and control forces in a digital battlefield. However, the DoD is continuously challenged with attracting and retaining a skilled cyber workforce; limiting vulnerabilities and points of attack to its thousands of systems and networks; developing, testing, and using cyber capabilities; and integrating cyberspace operations into command plans.

The DoD's cyber missions require collaboration with foreign allies and partners. The DoD seeks to build partnership capacity in cybersecurity and cyber defense, and to deepen operational partnerships where appropriate. The DoD is focusing its international engagement on the Middle East, the Asia-Pacific, and key NATO allies.

Building and Retaining DoD's Cyber Workforce

To address the cybersecurity challenge, the DoD must attract and retain a cyber workforce with specialized skills. In 2016, the GAO identified the shortage of cybersecurity professionals in the Federal Government as a high-risk area. Since the DoD began building the Cyber Mission Force in 2012 and fielding teams in FY 2013, it has created 123 of the 133 planned teams with approximately 5,000 of the 6,200 planned personnel. Of these 123 teams, 27 are reportedly fully operational and have supported DoD and other national missions to protect critical systems, networks, and infrastructure. But hiring and retaining these talented and skilled personnel is a difficult challenge for any Government agency, given the intense competition for these skills.

The DoD Cyber Mission Force, U.S. Cyber Command, and the Military Services have identified a strategy to build, develop, and increase the number of professions with unique skills to perform critical functions such as computer network defense. The strategy generally entails developing and using new military occupational specialties, ratings and designators within the Military Services, training and career development paths, and retention options to bolster critical skills and improve the cyber workforce.

The DoD OIG issued a classified report in 2015 concluding that the Services faced continued challenges in fielding Cyber Mission Force teams. Among other actions, the DoD OIG recommended revising or developing fielding strategies and expanding training capacity to build Cyber Mission Force teams. Since the issuance of that report, the Deputy Secretary of Defense and the Commander, U.S. Cyber Command, stated that the DoD was attracting and recruiting a cyber workforce at a faster pace because of changes that gave the DoD enhanced authority to hire critical cyber professionals.

With regard to oversight of information technology systems and building the cyber workforce, the OIG will continue to conduct oversight in this challenging area. In FY 2017, the DoD OIG has ongoing or planned audits that will determine whether the:

- National Security Agency implemented appropriate controls to protect its systems, networks, and data from insider threats;
- combatant commands integrated offensive and defensive cyberspace operations into command plans;
- U.S. Cyber Command and the Military Services integrated the National Guard and Reserve Components in the Cyber Mission Force;
- Military Services and Defense Information Systems Agency effectively implemented Joint Regional Security Stacks as part of its Joint Information Environment initiatives
- Army secured electronic health records;
- DoD Components developed and tested contingency plans to minimize disruptions to operations;
- Military Services implemented approved and secure physical access control systems at DoD facilities and installations; and
- DoD effectively and appropriately shared cyber threat indicators within the Federal government.

In sum, although the DoD has taken steps to increase cybersecurity through offensive and defensive operations and build its Cyber Mission Force, significant challenges remain. The DoD needs to continue to focus in areas such as maintaining a skilled cyber workforce, developing and using cyber capabilities, and integrating cyberspace operations into command plans. The challenge for cybersecurity is that adversaries and defenders constantly innovate and adapt capabilities, and it is a continuous effort to protect DoD's systems and networks from increasingly sophisticated cyberattacks. The DoD must develop and evolve its tactics, techniques, and technology and build and retain a highly skilled cyber workforce to detect and respond to increasingly sophisticated threats, whether defensively or offensively.

5 – Improving Financial Management

Financial Auditability Eliminating Improper Payments

Financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support operating, budgeting, and policy decisions. DoD financial management covers a complex array of financial topics— including procurement, inventory, payroll, asset management, and real property—across a very complex organization structure. However, the DoD is the only Federal agency that has never undergone a full financial statement audit. Moreover, the DoD financial statements are the major impediment to a successful audit of the U.S. Government.

The DoD financial statements have not been ready for audit since the DoD began preparing financial statements in the early 1990s. Neither the DoD as a whole nor its Military Services have been able to provide auditors sufficient evidence to undergo a financial statement audit.

The DoD is required by the Chief Financial Officers Act of 1990 to achieve a full financial statement audit covering its budget, assets, and liabilities. Public Law 111-844 specifically requires DoD to have audit-ready financial statements by September 30, 2017. In addition, the Office of Management and Budget Circular No. A-123 defines management's responsibilities for enterprise risk management and internal control. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal controls into existing business activities and as an integral part of managing an agency. Enterprise risk management is a key element of reaching financial auditability and the DoD continues to be challenged by these requirements.

Financial Auditability

Providing auditable financial statements is critical for ensuring that programs are working and funds are being used properly. Unreliable financial information makes it difficult to accurately develop and execute budgets or to determine the effectiveness and efficiency of military operations. DoD financial management challenges make it difficult to see potential waste, mismanagement, and cost overruns. Financial management procedures are often manual and limit the DoD's ability to develop repeatable processes that could be achieved through well- designed automated solutions.

If the DoD can achieve a favorable opinion on its financial statements, these improvements can also help management make better decisions when predicting operational requirements. For example, the DoD OIG found that some budget submitting offices in the Navy could not support the validity and accuracy of obligations during its triannual review of unliquidated obligation and unfilled customer orders in May 2014. This inability to support the obligations did not provide the

Navy with the assurance that its financial reporting accurately reflected the status of its obligation and may have lost the opportunity to use funds for other purposes.

Current State of Audits

DoD OIG audits continue to show a lack of supporting documentation for account balances and system data that are not reliable, accurate, or timely. Asset information, such as inventories, continues to show problems with valuation, location, and counts that can result in operations placing orders for new parts or equipment even though there are sufficient supplies on hand.

Lack of well-designed system interfaces also hamper the DoD's ability to compile accurate and timely financial and program information. For instance, the DoD OIG has found that the DoD lacks adequate internal controls over the disbursement and obligation of appropriated funds, key reconciliations to "balance the checkbook," appropriately valuing its assets, improving controls in key financial systems, and preparing unsupported journal vouchers used to force accounting entries in the financial statements to match. The DoD OIG's July 2015 audit report summarizing prior audits of DoD financial management highlighted these material internal controls weaknesses and identified that the corrective action for over 130 recommendations still needed to be implemented. Some recommendations were over 4 years old.

The DoD OIG also performed a series of audits on improvements needed in DoD's management of suspense accounts. These suspense account audits highlighted that the DoD could not account for all of its transactions on the DoD's financial statements. Suspense accounts are designed to temporarily hold funds that belong to the Federal Government that do not have enough accounting information to immediately post the transaction to the proper financial statement.

However, DoD did not have controls in place to accurately record suspense account balances on the proper component-level financial statements or clear suspense account transactions and incorrectly recorded collections from revenue-generating programs, service member tax withholdings. In July of 2016, the DoD OIG reported that the Army did not adequately support trillions of dollars in journal voucher adjustments on its FY 2015 financial statements and that it materially misstated its inventory by millions of dollars. The value of unsupported journal vouchers continue to limit the reliability of the financial accounting information for decision makers who need to know whether programs are working and funds are being used properly. Inaccurate inventory information also limits DoD's ability to ensure materiel and equipment is available to for operational readiness.

Corrective Actions Taken by the DoD

Although DoD plans to conduct its full financial statement audits beginning October 1, 2017, as required by law, several key challenges continue to face the DoD when preparing for the audits. To address these challenges, the DoD is leading enterprise-wide initiatives that seek to support audit readiness or improve overall financial management. The DoD continues to update the Financial Management Regulation and issue policy memorandum to implement accounting policies and better ensure sustainable, repeatable, and standard processes. It also established formal governing bodies to emphasize the importance of DoD business and financial operations and achieving audit readiness. The DoD has also created working groups to ensure that solutions to its financial impediments comply with accounting standards and can pass auditor testing. DoD leaders are closely monitoring its progress.

What is Left to Do – Auditor's Perspective

Achieving audit readiness by September 30, 2017, will be a difficult challenge. These challenges cut across DoD Components and require DoD-wide changes to policies, procedures, and regulations. The major impediments to auditability require the DoD to improve and in some cases change its way of doing business. Long-standing business processes that have supported DoD missions are not always sufficient for an audit and must be transformed. For example, audits conducted by independent public accounting firms of the Services' FY 2015 Schedule of Budgetary Activity cited more than 700 combined findings and recommendations that revealed individual and systemic issues that resulted in unfavorable opinions on the Schedules.

Correcting material weaknesses and significant deficiencies that have been identified by public accounting firms should be the first priority of the Military Services. The DoD also needs to develop sustainable and repeatable processes to better respond to audit requirements and provide the best supporting documentation for sampled transactions.

To achieve and sustain audit readiness, the DoD must also focus on its high-risk areas such as the ability to eliminate the use of journal vouchers as a means of addressing unsupported accounting transactions. The DoD should also consider further consolidating the financial management systems throughout the DoD. The sheer number of business and financial systems is staggering when compared to other Federal agencies, and the level of effort and cost of ensuring all systems are audit ready is significant. DoD needs to expedite the retirement of legacy systems and ensure that remaining systems are interfaced appropriately. These systems should capture and process timely and accurate financial and program data that decision makers can rely upon to ensure programs are working and funds are being used properly.

The DoD's financial management environment is decentralized and consists of hundreds of systems processing transactions reported in the financial statements. Because the financial management processes lack adequate controls to support such a complex and convoluted structure they must eliminate systems and continue to develop and document adequate controls that comply with accounting standards.

Achieving audit readiness and improved financial statements requires leadership focusing attention on this effort. In this effort, leaders across the DoD are communicating that audit readiness remains a DoD-wide priority. Secretary Carter and Deputy Secretary Work continue to emphasize the importance of improving DoD business and financial operations and achieving audit readiness. The DoD are also monitoring progress. For example, in March 2016, a senior leadership committee co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff reviewed the status of audit readiness. Each Military Department reported it was on track to be ready for an audit by September 30, 2017. The Deputy Secretary stressed the importance of making and sustaining improvements.

Yet, while the DoD plans to have 90 percent of DoD's total budgetary resources and 43 percent of total assets under audit in FY 2017, there are still critical capabilities and remediation efforts that need to be accelerated in order for full financial statement audits to begin in FY 2018.

Further, the DoD needs to address how to protect sensitive data while still presenting financial statements in compliance with U.S. GAAP. These challenges are magnified as the DoD is also facing continuous personnel and budgetary constraints as another fiscal year begins under a continuing resolution.

In addition, the DoD must be able to account for its assets reported on its Balance Sheet, including adequate support for how much assets cost, how much the DoD owns, and where the assets are located. In addition, audit success is closely linked to cash traceability, including proper management and accountability of all transactions to include fully reconciling financial transaction universes. Unsupported journal vouchers and unresolved differences between DoD and the Department of the Treasury are material and jeopardize achieving audit ready financial statements.

Without these improvements, the DoD financial statements will continue to remain unreliable and managers will not be able to rely on its accounting systems to make important management and resource decisions.

Improper Payments

Improper payments are defined as payments, including both overpayments and underpayments, that should not have been made or that were made in an incorrect amount. Reducing improper

payments is another important financial management challenge facing the DoD. Improper payments are often the result of unreliable data or a lack of adequate internal controls that increase the likelihood of fraud.

Recently, DoD OIG reports highlighted improper payments related Government travel charge cards. For example, in March 2016, the DoD OIG reported that the DoD Components did not take adequate actions to reduce estimated improper payments in the DoD Travel Pay program, as required by the Improper Payments Elimination and Recovery Act (IPERA). The DoD OIG reported that the DoD missed its improper payment reduction goals for 3 consecutive years. In addition, the GAO reported in June 2016 that the DoD did not submit proposals for reauthorization or statutory changes to Congress in response to 3 consecutive years of noncompliance with IPERA requirements in its Travel Pay program.

For the DoD FY 2015 Agency Financial Report, the DoD met five of the six requirements in accordance with the IPERA. Specifically, the DoD published a financial report; conducted program-specific risk assessments; published corrective action plans; published improper payment estimates; and reported improper payment rates of less than 10 percent. However, the DoD did not achieve its improper payment reduction targets for one of the eight payment programs with established targets. Not attaining reduction targets indicates that additional corrective actions are needed to reduce improper payments.

Overall, the DoD OIG found that the DoD has made progress in improving the identification and reporting of improper payments. For example, it has taken corrective actions to implement recommendations made by the DoD OIG to reduce improper payments in the DoD Travel Pay program and complying with IPERA, such as submitting remediation plans to address internal control deficiencies, and developing metrics and quality assurance goals related to IPERA reporting.

Additionally, two recent DoD OIG reports identified challenges with improper payments related to Government travel credit cards. A May 2015 report found that from July 1, 2013, through June 30, 2014, DoD cardholders had 4,437 transactions totaling $952,258, where they likely used their travel cards at casinos for personal use. In addition the DoD OIG identified 900 DoD cardholder transactions totaling $96,576 at adult entertainment establishments. An August 2016 report found that DoD management and travel card officials did not take appropriate action when notified that cardholders potentially misused their travel card. Specifically, DoD management did not perform reviews on sampled cardholders, did not take action to eliminate additional misuse, and did not review cardholder travel vouchers that indicated personal use. By reducing improper payment, DoD can use those funds to meet other critical operational needs.

6 – Protecting Key Defense Infrastructure

Installations and Energy
Space
Defense Industrial and Technological Base

Protecting key defense infrastructure, such as installations, space, and the defense industrial base, is a critical challenge for the DoD. The DoD must ensure that its installations worldwide are protected and sustained to meet operational mission requirements. The DoD must also maintain and protect its assets in space. In addition, the DoD needs to address supply chain vulnerabilities and its strategic competitors.

Installations and Energy

The DoD manages over 500 installations worldwide, consisting of nearly 300,000 buildings. It must ensure that each installation is maintained and sustained to support operational mission requirements. To accomplish this, the DoD is constantly prioritizing its military construction, sustainment, and recapitalization requirements. The DoD must meet these requirements, with constrained funding, while managing the security risks to installations and the challenge to contribute to mission readiness.

The growing need for military construction projects has increased the need for accurate and reliable justifications and cost estimates for military construction projects. The DoD has made progress in managing installations efficiently and economically. In particular, the DoD has increased the use of renewable energy and energy saving projects on DoD installations to provide energy security and to help the DoD comply with various energy mandates and goals. Some of the renewable energy and energy saving projects include improved lighting; high- efficiency heating, ventilation, and air conditioning systems; double-pane windows, solar and wind electricity, and new roofs.

In FY 2015, the DoD spent $16.7 billion to satisfy the DoD's energy needs. However, OIG audits show that DoD has not implemented sufficient controls to effectively monitor and oversee renewable energy and energy contracting. Specifically, a series of audits demonstrated that DoD does not have sufficient programs to ensure that energy savings performance contracts and utility energy services contracts were providing cost savings. In some cases, the DoD spent millions on projects that may not have achieved sufficient energy savings to pay back the utility company's investment as required or to support payments to the contractor based on estimated guaranteed future annual cost savings.

In addition, energy availability directly affects the capabilities of weapons platforms, facilities, and equipment, while remaining a substantial expense for the DoD. Energy is an important part in

sustaining worldwide military operations because energy is used by installations, ships, aircraft, and combat vehicles. Some of the DoD's largest challenges are supporting energy innovation in current operations and integrating energy considerations into force development. Furthermore, the DoD is striving to meet the President's goal to produce or procure not less than 25 percent of its total energy consumption from renewable sources by 2025.

Space

The DoD's assured access to space and its ability to maintain space control is a significant management challenge. Space control seeks to support freedom of action in space and, when necessary, defeat adversary efforts that interfere with or attack U.S. or allied space systems and negate adversary space capabilities.

Currently, with regard to assured access to space, the Air Force is attempting to reduce the cost of national security launches and eliminate the reliance on Russian-made RD-180 engines. To accomplish these objectives and to move to a new generation of launch vehicles, the Air Force must certify two new launch vehicles being developed by the United Launch Alliance (ULA) and Space-X. In addition to access to space, the DoD needs to maintain the long-term dominance of its space technologies and capabilities. In September 2016 testimony before the Senate Armed Services Committee, for example, General Hyten emphasized the importance of operations in space, "In space, threats continue to grow.as potential adversaries attempt to counter what has become a critical advantage for our Nation and our allies."

Recent OIG space-related projects include ongoing quality assurance inspections of ULA and Space-X launch vehicle manufacturing and test operations. The OIG plans to conduct other space-related oversight projects in the future.

Defense Industrial and Technology Base

The DoD draws from a large network of global suppliers for its equipment and support needs. For example, in fiscal year 2014, the DoD managed over 4.7 million parts that are used in communications and weapon systems, at a cost of over $96 billion. In many cases, this has allowed U.S. firms to harness the creativity of the global market. However, these supply chains create vulnerabilities and are subject to manipulation by strategic competitors.

One of the vulnerabilities within the global supply chain is the widespread existence of counterfeit parts. Counterfeit parts can, for example, delay missions, affect the integrity of systems, and ultimately endanger the lives of service members. Almost anything is at risk of being counterfeited, including microelectronics used in fighter jets and missile guidance systems, fasteners used in aircraft, and materials used in engine mounts.

In response to this risk, in 2013, the DoD created policy to prevent the introduction of counterfeit into the supply chain, as well as testing and other means by which to detect counterfeit materials that may have already entered it. The DoD also issued regulations, as required by the 2012 National Defense Authorization Act, that require DoD personnel and contractors to report suspected counterfeit electronic parts to a cooperative activity between Government and industry. Called the Government-Industry Data Exchange Program, this program allows Government and industry participants to share information on nonconforming parts, including suspect counterfeit parts, through a web-based database. The act also requires that contractors develop and maintain systems to detect and avoid counterfeit electronic parts.

The GAO recently reviewed DoD's efforts to address vulnerabilities to counterfeit parts in its supply chain. The GAO found several aspects of DoD's implementation of its mandatory reporting for suspect counterfeit parts have limited its effectiveness as an early warning system. The GAO also concluded that, without proper oversight ensuring that the reporting requirement was consistently applied, the DoD could not ensure it is effectively managing the risks associated with counterfeit parts.

Investigation of product substitution, including counterfeit, defective or substandard products, is one of the top investigative priorities of the DCIS. Product substitution disrupts readiness, wastes economic resources, and threatens the safety of military and Government personnel and other end users. As of September 30, 2016, the DCIS had 159 active product substitution cases that represented approximately 10 percent of active investigations. In FY 2016, the DCIS' product substitution investigations resulted in 5 arrests, 17 criminal charges, 11 convictions, and over $41 million in recoveries for the Government.

A recent DCIS product substitution investigation led to the conviction of an individual, who imported thousands of counterfeit integrated circuits from China and Hong Kong and resold them to U.S. customers, including contractors who supplied them to the DoD for use in nuclear submarines. The perpetrator pled guilty to conspiring to traffic in counterfeit military goods, and was sentenced to 37 months imprisonment, and ordered to pay $352,076 in restitution to the 31 companies. In addition, the perpetrator was issued two forfeiture money judgments totaling over $1.8 million. A separate DCIS investigation found that a company supplied nonconforming mechanical parts to the Defense Logistics Agency for use on various weapons systems, including aircraft, vessels, and vehicles. The majority of these parts were critical application items, which are items essential to weapon system performance or operation, or the preservation of life or safety of operating personnel. A jury convicted the company's president of mail fraud and false claims. The individual is awaiting sentencing and was debarred, along with the company, from Government contracting for a period of 3 years.

In summary, the DoD has made progress in installation and energy management, and it has recognized the urgency of maintaining control of space. It must also focus on preventing the introduction of counterfeit parts in the supply chain, which is a difficult and widespread challenge.

7 – Developing Full Spectrum Total Force Capabilities

Structure and Posture of the Force and Building Diverse Capabilities Despite Budget Pressures

Chemical, Biological, Radiological, Nuclear, and Explosives Issues

Designing, building and posturing a total force, active and reserve, capable of executing a wide range of missions across the full spectrum of potential conflict is a continuous challenge for the DoD. Increasingly diverse threats and capability requirements combined with significant budget pressure requires the DoD to make difficult strategic choices in developing its total force.

For much of the last decade, the DoD has focused on capabilities needed for combatting violent extremists and building partner capacity in Afghanistan, Iraq, and, most recently, Syria. As noted in previous challenges, violent extremism and terrorism continue to threaten the United States and its allies. At the same time, Russia, Iran, North Korea, and China are threatening U.S. strategic interests and the stability of regions throughout the world. Other countries and non- state actors continue attempts to obtain and upgrade modern conventional weapons, advanced technologies, and weapons of mass destruction.

As the DoD builds on the new capabilities it has developed in the fight against violent extremists, it also must refocus on capabilities necessary to counter current and future strategic threats. This refocus extends across all domains (land, sea, air, space, and information) and heightens competition for resources, the need for new ways of thinking to extend U.S. military dominance, and the critical importance of optimizing the value of DoD capabilities and components across the full spectrum of conflict.

The most recent DoD initiative to maintain U.S. military superiority over its adversaries, primarily China and Russia, is its Third Offset Strategy. Announced in FY 2015, this strategy seeks to develop and employ new technologies and operational concepts to offset adversaries' investments while increasing U.S. capabilities in a way that it cost effective. With its emphasis on research and development, experimentation, war gaming, and faster adoption of new technologies, the Third Offset Strategy is a timely and promising initiative that will benefit from OIG oversight.

In addition to pursuing innovative technologies and operational concepts, the DoD continues to assess the size and mix of its total force to maintain an optimal mix of active and reserve forces that can defeat our enemies and defend the homeland. For example, the DoD is reviewing how it will train and use Active and Reserve Components and where to position its personnel and assets

throughout the world to ensure it has adequate total force capability. This is not a new issue. In 2007, the Secretary of Defense wrote that the DoD was assessing options on how best to support global military operational needs, including whether the DoD has the right policies to govern how Reserve, National Guard, and Active Component units are used. In 2008, the Secretary issued guidance emphasizing that the Reserve Components provide operational capabilities and strategic depth to meet U.S. defense requirements across the full spectrum of conflict and that the military services need to better integrate Reserve Component capabilities into their respective total force structures. The Services efforts to assess the right balance of active duty, reserve, and National Guard resources are discussed below.

In May 2011, the Secretary of the Air Force discussed reshaping the structure of the Air Force in the face of enduring budget constraints. At that time, the Air Force had 144 initiatives across the service aimed at identifying efficiencies and the right mix of personnel, technology, and modernization. In 2014, Congress also established the National Commission on the Structure of the Air Force to recommend how the force structure should be modified to meet present and expected mission requirements within available resources. The Commission's report, issued in January 2014, provided recommendations to rebalance Active, Reserve, and Air National Guard components; increase the end strength of the Reserve components; and increase regular, periodic, and predictable use of Reserve component forces.

The National Commission made recommendations to increase the number of "associate units" between Active and Reserve components and to create a single integrated chain of command for these associate units. Acting on these recommendations in the report, the Air Force intends to reach initial operational capability in its Integrated Wing Pilot Program in FY 2017. This program will align Active and Reserve components under a single chain of command to leverage the strengths of both components and meet mission requirements more efficiently and effectively.

The FY 2015 National Defense Authorization Act established the National Commission on the Future of the Army to evaluate, in part, how Army National Guard and Army Reserve personnel are integrated into the Total Force. DoD and Army policy directs the Army to ensure total force policies encourage the optimum use of active and reserve component personnel and to organize, man, train, and equip the Army, Army National Guard, and Army Reserve as "an integrated, operational Total Force." During a speech on August 3, 2016, the Secretary of Defense stated, "The days of the National Guard serving exclusively as a strategic reserve are over." He added that the Guard is an "indispensable component of the Total Force," whether in day-to-day activities or large-scale operations. Army National Guard officials acknowledge that this new role will require a shift in the mindset of Guard unit leadership and personnel.

As part of a series of audits on the readiness of military units, the DoD OIG is completing an audit of National Guard Armored Brigade Combat Teams training to perform unified land

operations—a full spectrum operations capability. Based on interim audit results, the DoD OIG issued a Notice of Concern to the Army National Guard regarding turnover within key leadership positions and methods used to assess and report readiness for some units. The DoD OIG also determined that training programs were not effective in ensuring whether units could attain and sustain mission proficiency. The DoD OIG recommended that the Army and the Army National Guard provide commanders clear guidance for managing training programs, maintaining unit cohesion, and ensuring assessments more accurately reflect training readiness.

During FY 2017, the DoD OIG will conduct an audit of personnel readiness reporting levels in National Guard units. Personnel readiness data, such as the type, number, rank, and status of personnel assigned to a unit, is critical information that leaders need to make informed decisions on whether units are available to deploy. As the role of the reserve components in DoD's total force continues to evolve, DoD's ability to rely on personnel readiness data provided by the Guard units will become increasingly important. The planned audit will focus on accuracy of reported personnel readiness levels at select Army National Guard and Air National Guard units.

The Navy is increasing its fleet from 280 ships at the end of FY 2016 to 308 ships in FY 2021. The fleet consists of aircraft carriers, submarines, surface combatants, amphibious ships, combat logistics ships, and support ships. The Navy's top shipbuilding priority is to replace the aging Ohio class ballistic missile submarines, which are a key component of the nation's nuclear triad. The Navy plans to build the first new Ohio-class submarine in FY 2021. Additionally, although the Navy is statutorily required to maintain 11 aircraft carriers, it has operated 10 carriers since the retirement of the USS Enterprise in 2012. Extended deployments of the remaining ships have placed stress on crews. The critical and costly carrier and submarine programs consume about half of the Navy's shipbuilding resources, affecting the Navy's ability to build ships of other classes. The Navy has identified additional amphibious vessel requirements and has a significant shortfall in small surface combatants. While prioritizing shipbuilding, the Navy is also taking steps to improve information warfare capabilities, invest in naval aviation, rapidly integrate unmanned systems, and bolster investments in advanced weapons. Filling capability gaps while maintaining the current fleet and meeting global operational and forward presence requirements is a significant management challenge for the Navy that requires objective oversight.

Regarding force size, the DoD's FY 2017 budget request includes a total force of 2,073,200 active, reserve, and guard soldiers. The following table shows the total force requests for each service in FY 2017.

Table. DoD Total Force Request for the FY 2017 Budget

	Army	Navy	Marine	Air Force
Active	450,000	323,100	182,000	317,000
Reserve	195,000	58,900	38,500	68,500
Guard	335,000	-	-	105,200
Total	**980,000**	**382,000**	**220,500**	**490,700**

This force size, the smallest in decades, increases the need for effective management, as well as comprehensive oversight to ensure the most effective and efficient employment of the total force.

For over 50 years, U.S. airpower superiority has been a core component of our full-spectrum total force capabilities. Each Military Service is experiencing challenges in maintaining air combat power advantage over our adversaries. After 25 years of near constant combat and use, DoD's fleet of aircraft is aging and in need of overhaul or replacement. Military aviators remain heavily engaged around the world, yet full-spectrum readiness and the size of the force remain a significant concern. To address these challenges, the DoD is acquiring new aircraft such as the MV-22 and the F-35 Joint Strike Fighter, as well as slowing the retirement of aircraft like the F/A 18 and A-10 through overhaul and sustainment efforts.

In 2013, the Army began its Aviation Restructuring Initiative in which it planned to cut its aviation force to achieve end-strength and budget-driven structure limitations. The initiative proposed to retire or reassign aircraft and deactivate aviation brigades. The goal of the Army's Aviation Restructuring Initiative is to protect modernization efforts and optimize the mix of Active and Reserve components. For example, the initiative transfers the Apache Helicopters from the Guard to active duty units and reassigns the H-60 from the active duty units to the Guard. In September 2016, the DoD OIG began an audit of the Army's modernization efforts related to the H-60 Black Hawk fleet.

Aging aircraft also has an impact on the training readiness of the aviators who have less equipment on which to train. In March 2016, the Senate Armed Services Committee specifically expressed concerns about whether Marine Corps aviators were conducting sufficient training and if squadrons had the appropriate number of aircraft to maintain training readiness and respond in crisis. As part of an ongoing series on the readiness of military units, the DoD OIG has initiated an audit to assess whether Marine Corps aviation squadrons have adequate aircraft capable of performing assigned missions and sufficient trained aviators to meet readiness requirements.

The DoD's efforts to improve active and reserve integration provide depth that increases the DoD's ability to protect U.S. interests in regions throughout the world such as the Asia-Pacific Region. In 2011, President Obama called for the United States to return its attention to the Asia-Pacific region and called for a rebalancing of forces in the area. In 2015, Secretary Carter stated that the DoD's roles in the Asia-Pacific rebalance are to:

- invest in future security capabilities such as a new long-range stealth bomber, a long-range anti-ship cruise missile, and rapid runway repair;
- field capabilities—like the Virginia-class submarine and F-35 Joint Strike Fighter developed over the last decade for use in the region;
- leverage new uses for existing technologies such as adapting the Tomahawk from a fixed, land-based target environment to use in a mobile maritime environment;
- adapt regional force posture to include the construction of new facilities and geographic distribution of equipment and personnel across the region; and
- reinforce alliances and partnerships through efforts such as security and technology cooperation and humanitarian and disaster relief.

To determine if units are equipped to execute their missions, the DoD OIG has audited the distribution of equipment across the Asia-Pacific region. Specifically, the DoD OIG conducted multiple audits on the ability of Military Services to effectively equip their units in the region. For example, the DoD OIG recently conducted a series of munitions inventory audits in the region to determine whether the Navy and Air Force had an accurate account of the type, quantities, and condition of its munitions. Two additional DoD OIG audits determined that Army and Marine Corps units in Korea did not have sufficient, properly maintained chemical- biological personal protective equipment and that units were not training to conduct operations under appropriate threat conditions. In FY 2017, DoD OIG will conduct a followup audit to determine whether Air Force commands have implemented corrective actions related to a 2013 DoD OIG audit on the stocking and distribution of expeditionary airfield resources and repair kits. These audits demonstrate that the U.S. Pacific Command preparedness for contingency operations remains a challenge. In addition, the DoD is transferring defense equipment to its international partners to enhance their military capabilities and enable their military forces to work with U.S. forces in deterring and defeating aggression. Under the Foreign Military Sales Program, the DoD sells advanced defense equipment, such as unmanned aircraft systems and radar systems, to international partners and conducts post-delivery monitoring to ensure transferred equipment is used for intended purposes established in international agreements. The DoD OIG recently announced the first in a series of audits to evaluate DoD's oversight of U.S. defense equipment transferred to international partners in the Asia-Pacific region. The audit will determine whether U.S. Pacific Command is conducting its Enhanced End-Use Monitoring Program to ensure that advanced defense equipment transferred to international partners is being used for intended purposes.

The DoD IG, as the Chairperson of the of the Interagency Coordination Group of Inspectors General for the Guam Realignment, issues an annual report on the programs and operations on Guam funded with military construction appropriations. The annual report also summarizes oversight efforts of the DoD OIG, the Department of the Interior, and the Service-level audit agencies related to these funds. In addition to its role on the Interagency Coordination Group, the DoD OIG also continues to provide oversight through audits related to the realignment. For example, in 2015, the DoD OIG reviewed the administration of the Guam Multiple Award Construction Contract, a $4 billion contract issued by the Navy for military construction projects related to the relocation of Marines to Guam. The report identified weaknesses in the Navy's contract administration processes, which led to the construction of facilities that did not meet mission and regulatory requirements.

Where forces are deployed throughout the world is another critical issue for maintaining full- spectrum total force capabilities. Evolving threats throughout the world, as discussed previously, affect these key strategic decisions. For example, in recent years, the U.S. and NATO allies across Europe are increasingly challenged by political instability in the region, often spurred by Russia. However, following the dissolution of the Union of Soviet Socialist Republics and the Warsaw Pact, the DoD reduced its force posture and closed bases in Europe. In light of recent conflicts and instability, the DoD has committed to supporting U.S. interests and allies in the region through increased presence and multinational training events and exercises.

From FY 2015 to FY 2017, the DoD budgeted nearly $5.2 billion to fund the European Reassurance Initiative. Through the initiative, the DoD seeks to reassure our NATO allies and bolster the security and capacity of our partners. The initiative consists of increasing the presence of U.S. forces in Europe through stepped-up rotations and continued deferral of some previously planned force reductions or potential force restructuring initiatives. Specifically, the Army is augmenting its presence through the rotation of stateside units. The Air Force is sustaining its current air superiority force structure in Europe and augmenting NATO's Baltic Air Policing mission. The Navy will continue its expanded presence in the Black and Baltic Seas.

To assess the effect of this initiative, in April 2016, the DoD OIG initiated an assessment of the effectiveness of the European Reassurance Initiative. This assessment will evaluate, among other matters, whether improvements have been made to European partner country infrastructure and whether U.S. and NATO forces have increased force responsiveness, interoperability, and sustainability. The DoD OIG also recently announced an audit to determine whether the U.S. European Command is integrating offensive and defensive cyberspace operations into its operational and contingency plans.

Chemical, Biological, Radiological, Nuclear and Explosive Issues

Countering the potentially catastrophic effects of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons is a key component to the challenge of maintaining full- spectrum total force capabilities. DoD's challenge in this area is two-fold. The DoD must protect military personnel from CBRNE threats and train them to carry out military operations under CBRNE threats or hazards. The DoD must also ensure proper handling of the CBRNE materials in its possession and protect the public from exposure. Adequately training and equipping the force to recognize, respond, operate, and recover from CBRNE attacks and hazards remains a challenge for the DoD and an oversight priority for DoD OIG.

Hostile actors, including terrorists and supporters of terrorists, are seeking to acquire weapons of mass destruction and materials to construct weapons of mass destruction. This poses a significant and potentially catastrophic threat to the United States and its allies. CBRNE threats include the intentional employment of, or intent to employ, weapons or improvised devices that produce CBRNE hazards. To counter this threat, the DoD must enable its forces to deter, prevent, protect, mitigate, respond, and recover from CBRNE threats and effects. Achieving this mission requires, in part, equipping the force to successfully conduct military operations under CBRNE threats and effects.

As previously discussed, the DoD OIG recently conducted two audits that identified weaknesses in CBRNE equipment and collective training for Army and Marine units in Korea. Because of concern that similar equipment and training weaknesses may exist in other commands, the DoD OIG intends to assess whether U.S. Special Operations Command has sufficient quantities and types of CBRNE equipment on hand. The audit will also evaluate if personnel are adequately trained and CBRNE qualified.

The DoD OIG is also conducting a series of projects concerning the security of and accountability for CBRNE materials in DoD's possession. In April 2016, the DoD OIG issued a report on the evaluation of controls over biological materials in DoD Component laboratories.

The evaluation highlighted weaknesses in the oversight of several DoD laboratories including inconsistent guidance and inspection policies across the Military Services and inadequate training of officials conducting inspections of the facilities. The DoD OIG is also completing an audit that will address the controls over chemical surety materials at DoD installations and laboratories. The review will address the security controls over these materials including accountability for the chemical agents, access controls to facilities, and vetting of personnel who have access to and protect chemical materials. In 2017, the DoD OIG plans to conduct a review of the Nuclear Surety Program that will review the controls over personnel with access to or responsibility for safeguarding nuclear materials. The DoD OIG continues to oversight of the governance and

sustainment of the U.S. nuclear weapons enterprise. A 2016 OIG review detailed weaknesses and open recommendations from the last 5 years of DoD OIG nuclear reports, such as weaknesses in guidance for implementing Presidential and DoD directives**,** requirements for nuclear weapon security and employment, manning and training of theater nuclear planners, budget or funding priority to sustain nuclear command and control capabilities, and logistics and parts issues to sustain

the Minute Man III missiles. In addition, a September 2016, DoD OIG report documented a lack of interdepartmental coordination on intelligence requirements for the nuclear enterprise.

Other reviews related to DoD's capabilities are ongoing. For example, the DoD OIG is currently reviewing the National Airborne Operations Center's ability to sustain its mission with the E-6B aircraft and evaluating the DoD's ability to organize, train, and equip explosive ordnance disposal teams that support the DoD's nuclear weapons mission. In FY 2017, the DoD OIG plans to examine the availability and reliability of the E-6B program (airborne command, control, and communications), the sustainment of nuclear ballistic missile submarines, and the ability of the nuclear detonation detection system to meet its DoD requirements.

In short, the DoD has recognized the importance of continually assessing and modifying its force structure and capabilities to counter evolving strategic threats, and this effort remains a continuing management challenge, particularly given growing pressure on resources.

8 – Building and Maintaining Force Readiness

Equipment Accountability and Reset Suicide Prevention Healthcare—Cost, Fraud, Access to Care Talent Management, Force of the Future

Building and maintaining the readiness of the current force to execute its diverse missions is one of DoD's core challenges and responsibilities. The DoD must ensure its forces are manned, trained, and equipped to deter and defeat our adversaries and to protect U.S. interests at home and abroad.

The DoD faces the challenge of rebuilding readiness after 15 years of continuous deployment. DoD leaders have stressed the need to balance current readiness against modernization and future force development to ensure forces can prevail against current and future threats. To maintain force readiness, the DoD needs to provide adequate equipment and also ensure the return of costly serviceable equipment from overseas deployments. In addition, the DoD must provide quality health care for members of the Military Services and their families, focus on suicide prevention, and recruit and retain high quality military and civilian personnel.

Equipment Accountability and Reset

An important aspect of readiness is the availability and functionality of the equipment for both training an operational needs. Properly accounting for equipment protects taxpayer money and allows DoD to appropriately and promptly respond to new contingencies worldwide. It also ensures that needed DoD equipment is not left behind, whether it is rolling stock or nonrolling stock. Rolling stock refers to vehicles such as tactical vehicles, ambulances, and wrecker trucks. Nonrolling stock refers to items such as generators, weapons, and radios. After equipment is returned to the United States, it is reset or refurbished so that it can be re-issued to military personnel for training and deployment.

Property accountability has been a continuous challenge for the DoD in both Iraq and Afghanistan. At its peak in 2012, more than 18,000 pieces of DoD equipment were used in Afghanistan, with limited accountability. As a result, multiple DoD OIG reports documented the loss of hundreds of millions of dollars in equipment, including thousands of sensitive items. For example, a 2014 report concluded that the Army reported accumulated losses of $586.8 million in equipment in Afghanistan for 1 year. An OIG audit also found poor security, limited qualified property accountability experts, and the lack of urgency when reporting inventory losses in a timely manner in Afghanistan. DoD OIG audit reports also recommended improvements to the security and storage of equipment in Afghanistan, Kuwait, and the United Arab Emirates**,** particularly with sensitive items such as communications equipment.

Suicide Prevention

Suicide continues to be a public health concern for America and its military veterans. Historically, the suicide rate was lower in the military than the civilian population. However, in 2008, for the first time, the suicide rate in the Army exceeded the age and gender adjusted rate in the civilian populace and continued to be higher through 2015. Active Component suicides slightly decreased from FY 2014 through FY 2015, but Reserve Component suicides increased. According to recent DoD data, there were a total of 478 suicides in 2015.

The DoD has developed and promoted prevention policies, practices and programs to attempt to reduce military suicide. For example, the Defense Suicide Prevention Office (DSPO) leads working groups of representatives from the Services, the Office of the Assistant Secretary of Defense for Health Affairs, and other stakeholders on expanding access to behavioral health care for service members. The DSPO also implemented the DoD Strategy for Suicide Prevention in 2015 that attempts to coordinate suicide prevention efforts across the DoD. For example, the DSPO has published and distributed guides to military family members on suicide warning signs, risk factors, and actions to take in a crisis. DSPO also sponsors research initiatives and training that address gaps in suicide prevention and resilience policies and practices.

In addition, the DoD collaborates with the Veterans Administration to develop suicide prevention and intervention policy. For example, in June 2103 the DoD and Veterans Administration jointly developed the Clinical Practice Guideline, "Assessment and Management of Patients at Risk for Suicide," which recommends best practices for assessing and managing the risk of suicide among active duty military and veterans.

However, shortcomings in DoD suicide prevention efforts remain. A September 2015 DoD OIG report found that DoD lacked a clearly defined governance structure and alignment of responsibilities for the Defense Suicide Prevention Program. In addition, the report identified the lack of clear processes for planning, directing, guiding, and resourcing to effectively develop and integrate the Suicide Prevention Program within the DoD. In response to DoD OIG recommendations, the DSPO issued and implemented the 2015 Strategy for Suicide Prevention to coordinate suicide prevention efforts across the DoD. In response to another OIG report, the DSPO developed and is in the process of issuing guidance for data collection and reporting on suicide events that will also address DoD suicide prevention efforts.

To continue monitoring suicide prevention efforts, the DoD OIG will conduct an evaluation of DoD Suicide Prevention Policy Dissemination and Implementation.

Health Care

Providing quality health care for members of the Military Services and their families remains a challenge that is critical to force readiness. The Military Health System must provide care for over 9 million beneficiaries within fiscal constraints, while facing increased user demand and inflation. These challenges make cost control difficult. Over the last decade, health care costs in the United States have grown substantially, and Military Health System costs have been no exception. The DoD FY 2014 appropriations for health care were $32.7 billion, an increase of about 80 percent since FY 2005. Appropriations have almost tripled since the FY 2001 appropriation of $12.1 billion. In its FY 2017 budget, the DoD requested $33.8 billion for the Defense Health Program.

The DoD faces additional health care challenges such as preventing health care fraud, containing costs, and ensuring access to quality care. Health care fraud is another one of the top investigative priorities of DCIS. The DCIS has many open health care criminal investigations.

As of September 30, 2016, DCIS had 492 open health care cases that represent approximately 30 percent of DCIS's open investigations. In FY 2016, DCIS' health care fraud investigations resulted in 45 criminal charges, 34 convictions, and over $763million in recoveries for the Government. In FY 2016, DCIS' health care fraud cases have resulted in 32 criminal charges, 16 convictions, and over $380 million in recoveries for the Government.

As noted above, the DoD continues to struggle to contain costs in TRICARE programs. As one example affecting the rise in costs, the TRICARE Pharmacy Program experienced a dramatic rise in the receipt and payment of compounded drug prescriptions. Compounding pharmacies combine, mix, or alter two or more ingredients to create a customized medication for patients. From October 2014 to April 2015, payments for compound drugs increased from $84 million to $550 million per month, or 555 percent over the 7-month period. However, much of the increase was based on fraudulent activity. The DCIS opened 133 investigations relating to fraud by compounding pharmacies**,** many of which addressed allegations of health care kickbacks between the pharmacies, the marketers of the drugs, and the prescribing physicians. Often, the marketers used "pyramid schemes" to recruit individuals to promote the medications, and they often contacted TRICARE beneficiaries using direct marketing techniques. Frequently there was no doctor-patient relationship between the prescribing physicians and the beneficiaries, which is a requirement to bill under the TRICARE Program. Additionally, the majority of these fraudulent prescriptions were for creams that supposedly treated generic conditions such as pain and scarring.

A joint DCIS and FBI investigation led to the indictments of two individuals associated with a Texas-based company that marked compounded pain and scar creams to TRICARE beneficiaries on behalf of compounding pharmacies. The individuals were indicted on various health care fraud and other charges. The indictment alleged that defendants paid kickbacks of $250 per month to TRICARE beneficiaries for each compounded prescription they obtained, and paid physicians $60 for each compounded pain or scar cream they prescribed. The loss to TRICARE from their alleged scheme exceeded $65 million. The indictment contains a forfeiture allegation which would require the defendants, upon conviction, to surrender property traceable to the offenses including four homes, 18 bank accounts, and 21 cars and trucks, two motor coaches, and a boat. The investigation remains ongoing. A separate DCIS compounding pharmacy investigation resulted in a company paying DHA approximately $8 million to resolve allegation that it violated the False Claims Act by billing the TRICARE Program for compounded prescriptions that were not medically necessary and were not reimbursable.

While most of DCIS' compounding pharmacy investigations remain ongoing, they have already resulted in 38 criminal charges, four convictions, over $300 Million in seized assets, and over $90 million of recoveries.

In May 2015, DHA implemented new controls to reduce payments for compound drugs from $497 million in April 2015 to approximately $10 million in June 2015. The DoD OIG reported in July 2016 that while the controls were effective in reducing costs for compound drugs, additional controls were necessary to prevent reimbursement for certain non- covered compound drug ingredients. DHA concurred with the recommendation and is taking action to improve controls.

In addition to controlling health care costs, the DoD should improve collections for services provided at military treatment facilities. The DoD OIG issued five reports from August 2014 through April 2016 and concluded that military treatment facilities did not actively pursue collections from non-DoD beneficiaries for 120 accounts, valued at $11.3 million, of the 125 accounts the DoD OIG reviewed. Also, the military treatment facilities did not appropriately transfer funds to the U.S. Treasury for 114 delinquent accounts, valued at $13.4 million, of the 125 accounts the DoD OIG reviewed for collection.

The DoD OIG is also planning to review whether DoD is adequately meeting quality of care and patient safety standards for DoD service members and beneficiaries.

Talent Management, Force of the Future

The DoD is the nation's largest employer, with over 1.3 million men and women on active duty, 700,000 civilian personnel, and 800,000 personnel serving in the National Guard and Reserve forces. The DoD must remain competitive in its challenging efforts to recruit, develop, promote, and retain talented and skilled service members and civilians to serve the nation.

One example of this challenge is the reported shortage of Air Force drone and jet pilots. Air Force leadership has testified that the Air Force needs over 500 fighter jet pilots and approximately 500 drone pilots. Air Force leadership further testified that airlines have been recruiting Air Force pilots and that contracting firms have been offering high salaries to drone pilots. The GAO also testified that a series of interviews with drone pilots found low morale and that the pilots believed that a negative stigma was attached to their role. These challenges highlight the importance of talent management within the DoD.

In November 2015, the Secretary of Defense announced an initiative to examine DoD's civilian and military personnel practices. The goal of these efforts is to identify innovative and new ways to revitalize personnel and talent management systems and processes, which address changes in generations, technologies and labor markets. To meet the intent of this initiative, the DoD has identified approaches to modernize DoD personnel policies, procedures, and practices. In January 2016, the Secretary of Defense announced a second set of workforce reforms to improve the retention of service members and encourage public service.

In sum, the DoD continues to struggle in the areas of equipment accountability, suicide prevention, containing health care costs, and recruiting and retaining individuals. The OIG will continue to perform work in these areas in order to monitor the DoD's progress.

9 – Ensuring Ethical Conduct

Accountability and Integrity Whistleblower Issues
Sexual Assault Prevention and Response

Public trust and confidence in the DoD can be undermined by the small percentage of individuals who commit misconduct or crimes. High-profile scandals, corruption, waste, abuse of authority, acts of reprisal, or sexual assault involving DoD personnel are contrary to the DoD's high standards of integrity. The DoD must seek to minimize such misconduct and hold accountable anyone who commits it.

The Secretary of Defense and DoD leaders have repeatedly recognized this and stressed the need to make it a priority for the DoD to maintain ethical conduct and a culture in which honesty, accountability, respect, and integrity guide individual actions and decisions.

For example, in a memorandum dated February 12, 2016, "Leader-Led, Values-Based Ethics Engagement," the Secretary of Defense informed the DoD's leaders of his expectations regarding the importance of integrity and public confidence in Defense activities and its people. The Secretary directed that leaders, at every level, engage personally with their subordinates to discuss values-based decision making as set forth in the Joint Ethics Regulation to foster a culture of ethics and promote accountability, respect, and transparency throughout the DoD.

To pursue this objective, in March 2014 the Secretary of Defense established the position of Senior Advisor for Military Professionalism, which is currently filled by Rear Admiral Margaret "Peg" Klein. The Secretary charged Admiral Klein to work directly with the Service Secretaries and Chiefs regarding the DoD's focus on ethics, character, competence, and accountability in all activities at every level of command. In addition to regularly stressing positive examples of ethical leadership, in February 2016 Admiral Klein led the first DoD Professionalism Summit, which provided military leaders the opportunity to collaborate and share information on values- based leadership, character, and leadership development. The DoD OIG has engaged Admiral Klein and the Service IGs in regular meetings to share information on matters relating to senior official and whistleblower investigations, including the types of substantiated misconduct, outreach and training efforts, and efforts to improve the investigation of misconduct.

In another example of Service-level leadership, in April 2016 the Chief of Naval Operations (CNO) released the personal message he had provided to the Naval Flag officers and Senior Executive Service members emphasizing the Navy's core values of honor, courage, and commitment and the core attributes of integrity, accountability, initiative and toughness. The CNO emphasized to the Navy senior leaders that their personal conduct, and the example it sets, are essential to their credibility, as well as the overall integrity and efficiency of the Navy.

Investigations of Allegations of Senior Official Misconduct

Addressing misconduct when it occurs is essential to promoting ethical conduct throughout the DoD. It is important to hold individuals accountable if they have committed misconduct or clear individuals who have not. Therefore, investigations of misconduct should be conducted thoroughly and in a timely manner.

The DoD OIG and the Military Service IGs have received a large number of complaints and investigations involving allegations of senior official misconduct over the past several years. For example, from FY 2013 through FY 2015, the DoD and Military Service IGs received an average of 792 complaints and conducted an average of 260 investigations involving non-reprisal allegations against senior officials per year. Of those investigations, an average of 79 (30%) were substantiated each year. The types and severity of some of the substantiated misconduct is troubling. For example, recent investigations have substantiated serious misconduct by senior DoD officials such as accepting gifts from a Defense contractor, engaging in inappropriate relationships, and misusing Government resources.

Timeliness of investigations of misconduct remains a challenge. To pursue this objective, the Deputy Secretary of Defense asked the DoD OIG to lead a task force to examine ways to improve the timeliness of senior official investigations throughout the DoD. The DoD OIG teamed with the Military Service IGs and made recommendations to improve timeliness of investigations such as deploying a uniform administrative investigation case tracking system across the DoD, implementing a standardized system of investigative milestones among the Service IGs, providing uniform training for investigators, and monitoring the timeliness of investigations on a regular basis.

Despite these steps, timeliness of investigations remains a challenge throughout the DoD, given the increasing number of cases, the need for addressing allegations fully, and the limited level of resources devoted to these investigations.

Whistleblower Reprisal Investigations

Whistleblowers are important to exposing waste, fraud, and abuse in Government programs, and they are instrumental in saving taxpayers' money and improving the efficiency of Government operations. Whistleblowers must be protected from reprisals for protected disclosures. The DoD OIG is responsible for conducting and overseeing investigations when whistleblowers allege they have suffered reprisal. Without such investigations to protect whistleblowers from reprisal, individuals who can help save taxpayers' money—and possibly even save lives—may not report crucial information about wrongdoing and waste.

The DoD OIG and the Service IGs therefore seek to conduct thorough, fair, and timely investigations into allegations of whistleblower reprisal. It is a challenging task, particularly given the burgeoning whistleblower reprisal caseload and the flat level of resources available for such investigations in the DoD OIG and the Service IGs.

The DoD OIG has implemented improvements to the military whistleblower reprisal investigation program and is seeking to implement others. For example, the DoD OIG is seeking improvements throughout the DoD such as standardizing whistleblower reprisal investigations and implementing a DoD enterprise case management system for tracking administrative investigations.

In addition, in 2016 the DoD OIG established a dedicated team to investigate reprisal complaints stemming from whistleblowers who reported sexual assault. This action implemented one of the recommendations made by the Judicial Proceedings Panel in its "Report on Retaliation Related to Sexual Assault Offenses," which recommended that the DoD OIG investigate all complaints of professional retaliation related to sexual assault and ensure that these investigations are conducted by personnel with specialized training.

Sexual Assault Prevention and Response

Sexual assaults remain a significant challenge for the DoD. The DoD must focus on reducing sexual assaults and protect those who report sexual assaults from retaliation. According to the DoD Annual Report on Sexual Assault in the Military Fiscal Year 2015 issued on May 2, 2016, DoD's prevention programs focus on "reinforcing the cultural imperatives of mutual respect and trust, professional values, and team commitment to create an environment where sexist behaviors, sexual harassment, and sexual assault are not condoned, tolerated, or ignored." This report indicated that the DoD is working to address six key areas: 1) Advancing sexual assault prevention; 2) Encouraging greater reporting of sexual assaults; 3) Encouraging the reporting of sexual harassment complaints; 4) Improving response to male victims; 5) Combatting retaliation associated with sexual assault reporting; and 6) Tracking accountability in the military justice system.

According to the DoD annual report, fewer sexual assaults occurred in the military in 2014 than in 2006 when the DoD Sexual Assault Prevention and Response Program began, but a greater percentage of victims reported the crime. The DoD attributes changes in reporting behavior in part to the growth in sexual assault prevention and response programs since 2006. The annual report also stated that more must be done to implement an enduring culture change to enable service members to operate in a climate without sexual assault, including:

- creating the 2017-2021 Sexual Assault Prevention Plan of Action to advance the effectiveness of military sexual assault prevention programming; and
- launching the DoD Prevention Collaboration Forum to initiate greater coordination with

other DoD programs that address readiness impacting problems to leverage a unified approach to prevention—these programs include Family Advocacy Program, Defense Suicide Prevention Office, and the Office of Diversity Management and Equal Opportunity.

With respect to oversight of investigations of sexual assault allegations, the DoD OIG has a unit staffed with criminal investigators to oversee the DoD's sexual assault investigations. The DoD OIG also implemented overarching sexual assault investigative policy guidance to ensure uniform reporting and DoD investigations of sexual assaults. Since then, DoD policies have been updated to remain current of new legislative requirements, including the establishment of Special Victim Investigation Program implementing guidance for the investigation of all unrestricted reports of sexual assault with adult victims, crimes with child victims, and reports of domestic violence. Nevertheless, preventing sexual assaults, ensuring victims who report sexual assault do not suffer retaliation, and fully investigating allegations in a timely manner remain a continuing challenge throughout the DoD.

Public Corruption Investigations

Public Corruption involving the DoD and its personnel and programs wastes billions of tax dollars and can undermine public trust in the DoD. Yet, criminal misconduct by Government and contractor personnel in the DoD continues to pose a management challenge. The DCIS considers public corruption investigations to be among its highest priorities. In FY 2015, DCIS's public corruption investigations led to 52 criminal charges, 52 criminal convictions, and over $18 million in restitution and other monetary recoveries payable to the Government. The data for DCIS's work for FY 2016 is expected to be comparable.

A particularly compelling example of public corruption in DoD programs involves a decades long conspiracy of bribery and fraud by Glenn Defense Marine Asia PTE, LTD (GDMA). The investigation is ongoing and is being conducted jointly by DCIS and the Naval Criminal Investigative Service. The scheme involved the routine overbilling for goods and services that GDMA provided to Navy ships at various Asian seaports, including fuel, tugboat services, and sewage disposal. As of October 1, 2016, 15 individuals have been charged in connection with this scheme. A total of 11 of those individuals have pleaded guilty, including a Navy Rear Admiral, a Navy Captain, several other Navy officers and enlisted personnel, a NCIS special agent, GDMA's president, a former GDMA employee, and the GDMA corporate entity.

In summary, ensuring ethical conduct must be the focus of continual attention. The creation of a position such as the Senior Advisor for Military Professionalism to addresses ethical matters, and the emphasis placed on improving programs to prevent and investigate sexual assaults, demonstrate commitment at DoD's highest levels to address this challenge. However, an organization the size of the DoD will inevitably be faced with waste, fraud, abuse, assaults, and ethical misconduct by some employees and contractors. The DoD needs to remain focused on ensuring ethical conduct

and providing necessary resources and support for investigations to hold accountable those who do not uphold the high standards of the DoD.

10 – Promoting Continuity and Effective Transition Management

Changes of Presidential Administrations typically bring widespread turnover in DoD leadership positions as political appointees depart and potential delays occur in filling those vacancies.

According to the most recent edition of the Plum Book, in 2012 the DoD had 54 Presidentially Appointed, Senate-confirmed positions and 544 non-Presidentially Appointed Senate-confirmed positions potentially filled by political appointees.

While managing Presidential transitions is a challenging issue for all Federal departments and agencies, it is especially true for the DoD because of the national security implications. The importance of effectively managing the transition to a new administration is heightened now with the DoD engaged in two overseas contingency operations (OIR and OFS) and countering the evolving threats around the world. Gaps in leadership, delays in approving key decisions, and uncertainty about policy objectives can have significant effects on national security. For that reason, it is critical that the transition to new leadership be smooth, effective, timely, and seamless.

Moreover, on a regular basis, changes of leadership at all levels occur frequently throughout the DoD. Senior military leaders rotate positions every 1 to 3 years, as do military leaders at junior levels and forward deployed forces. This also presents a challenge for the DoD in ensuring continuity of operations.

Presidential Appointments

Expediting the appointment of incoming senior leaders within DoD is critical to the efficient and effective transfer of responsibility. During vacancies in leadership positions, career officials in acting positions are often responsible for managing their organizations. These officials are not able to make significant program or operational changes within their components.

In addition, comprehensive and accurate reporting on DoD programs, operations, and challenges is an important element for ensuring efficient and effective policy implementation by the incoming administration. DoD Components must be prepared to provide the incoming presidential transition staff with necessary briefings to assist in the identification of component- specific policy or program initiatives and challenges that require immediate attention. These comprehensive briefings should continue whenever new leadership arrives at the DoD. *Operations*

Access to DoD facilities and information, facilitation of communication between DoD and presidential transition organizations, and the provision of logistics support to the incoming

administration are also vital elements to achieving a successful Presidential transition. Focus needs to be given to areas such as access to information technology resources, full briefings on critical areas, and rapid processing of security clearances.

DoD leaders are focusing of transition planning. The Head of DoD Transition has been identified and the DoD Transition Task Force has been created and is meeting regularly to advance transition planning. As part of this effort, the DoD has already begun preparing a transition book and briefing materials for the transition teams and the new administration. The DoD transition book provides a high-level overview of each of the Defense agencies and Components. The book includes briefs on the functions, missions, structure, short and longer term deliverables, current budgets, and manpower.

The DoD OIG is also preparing a separate transition briefing book to provide a more in-depth view of the OIG organization and the work being conducted by our auditors, investigators, and evaluators.

Regular rotation of military leadership in the DoD is a well-established concept. Regular rotations expand an individual's functional, cross-functional, and leadership experience. Rotations also provide opportunities for military personnel to obtain depth and breadth of knowledge, broader perspective of the DoD's mission, and professional enhancement. However, these rotations result in frequent turnover for both senior and junior military leaders throughout the DoD and require careful planning and transition procedures. For example, requiring a strong management internal control plan, as well as documented processes and procedures, can ease these transitions and ensure minimal mission impact. Turnover is a perpetual challenge for the DoD, separate and apart from the significant turnover that accompanies a change of Presidential Administration.

In sum, the DoD must provide the new administration and its leadership, as well as the new officers that assume their roles during the frequent changes in leadership in the military ranks, with the knowledge and tools necessary to begin the work of leadership throughout DoD as soon as possible without gaps or delays.

DOD'S RESPONSE TO IG'S SUMMARY OF MANAGEMENT AND PERFORMANCE CHALLENGES FOR FY 2016

1 – Countering Global Strategic Challenges

Global Threats from China, Russia, Iran, and North Korea
Interagency Cooperation

The Department acknowledges the DoD IG's assessment of Countering Global Strategic Challenges.

2 – Countering the Terrorist Threat

Developing Partner Security Forces
Insider Threat

Developing Partner Security Forces

The Department acknowledges the DoD IG's assessment.

Insider Threat

The Department's resolve to institutionalize an effective insider threat program has not wavered. Significant progress has been achieved in establishing insider threat programs throughout the DoD Enterprise. New capabilities exist to enhance the screening of DoD personnel, control logical and physical access to DoD information and facilities, and share information vital to defeat insider threats. Although keeping pace with these advancements in policy is a challenge, issuances governing insider threat, physical, personnel, and industrial security are all pursuing refinements to keep pace with these advancements. DoD policy will soon be published to close the last recommendations from the Fort Hood shootings and implement measures that will assist commanders and supervisors with assessing risk and responding to impending threats. Physical security policies are being revised to address control procedures, badging and vetting criteria for all persons requiring access to DoD installations, facilities, and resources. As noted by the DoD IG, the National Industrial Security Program Operating Manual (Change 2) has imposed insider threat program requirements on DoD-cleared industry. The DoD Insider Threat Management and Analysis Center (DITMAC) has attained initial operating capability, receiving event reports from the Component analysis centers and full operational capability is projected in FY 2019. The linkage between the Component insider threat hubs and the DITMAC will further ensure that critical data regarding an adjudicative matter or security incident is reviewed quickly and swift action is taken if warranted. The DITMAC system, which facilitates this data exchange, has been accredited and continuous system improvements will enhance the analysis function and forge a more responsive and comprehensive risk assessment.

3 – Enabling Effective Acquisition and Contract Management
Linking Requirements to Strategic Military Plans
Contract Management and Oversight
Illegal Technology Transfer

Linking Requirements to Strategic Military Plans

As the IG notes, since 2010, the Department has instituted three iterations of Better Buying Power (BBP) initiatives that reflect our long-term commitment to continuous improvement of the defense acquisition system. Since then, the Department has seen a significant decline in the number of critical Nunn-McCurdy cost breaches from a high of 7 in 2009 to about 1 per year at present. Moreover, the growth of contracted costs for major programs has dropped during BBP from 9 percent in 2011 to a new 30-year low of 3.5 percent.

Recent major programs that project total funding reductions for development have risen from 27 percent in 2009 to 46 percent in 2015. Similarly for procurement, the numbers have risen from 39 percent to 77 percent.

The DoD has almost halted average incremental cost growth on major programs. Median biennial cost growth since 2011 on major active programs has run below 1 percent in development and production compared to highs near 6 percent at the turn of the century. Median total production cost growth on these active programs has run under 10 percent since 2010 and was under 5 percent in 2015 compared to 20-30 percent on a dollar basis in the early 2000s.

The Department remains committed to improving acquisition performance and will continue to emphasize reducing costs and establishing thoughtful business arrangements; ensure that requirements are fully supported and carefully reviewed prior to program initiation; and address program affordability as a systematic element of acquisition decision making.

Contract Management and Oversight

Contract Management continues to be a high priority for DoD leadership. Defense Procurement and Acquisition Policy (DPAP) is working aggressively to resolve the issues in the DoD IG's assessment by taking a number of steps to improve those identified issues including all aspects of the costing, pricing, and financing of its contracts. Many of the BBP initiatives are currently in process and are not meant to be one-time events, but a set of continuous learning and improvement approaches. Specific DPAP contributions to support BBP initiatives and improvements in contract management include:

On April 1, 2016, the Director of DPAP issued new DoD Source Selection Procedures (SSP) that rescinded the SSP issued on March 4, 2011 with exceptions detailed in the SSP. The guidance expands the discussion of both Tradeoff and Lowest Price Technically Acceptable source selection

procedures consistent with BBP initiatives, modifies evaluation methodologies, updates statutory and regulatory references, and includes best practices obtained through peer reviews.

On April 1, 2016, the Director of DPAP issued "Guidance on Using Incentive and Other Contract Types" developed as an element of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) BBP 3.0 - Achieving Dominant Capabilities through Technical Excellence and Innovation initiative. The analysis behind the 2014 Annual Report on the Performance of the Defense Acquisition System, published by the USD(AT&L)) on June 13, 2014, demonstrated that the use of cost-plus-incentive-fee and fixed-price-incentive Firm Target contracts was highly correlated with programs that achieved better cost and schedule performance outcomes. This guidance addresses, in a comprehensive way, the considerations our contracting and acquisition professionals should take into account when selecting and negotiating the most appropriate contract type for a given requirement.

To address negotiation of fair and reasonable prices for spare parts and other commercial items, the Director, DPAP issued "Guidance on Commercial Item Determinations and the Determination of Price Reasonableness for Commercial Items" on September 2, 2016. This memo provides guidance and previews policy changes that will implement the FY2016 National Defense Authorization Act provisions relating to commercial item pricing. The Department published 2016-D006 as a proposed Defense Federal Acquisition Regulation Supplement (DFARS) rule on August 11, 2016 to implement these provisions.

As a result of continuous emphasis and tracking of the Past Performance metric, the Department currently has an 85 percent compliance rate compared to the Federal Government Agencies' average of 61 percent. The Federal Acquisition Regulation (FAR) does allow contracting officers to document the reasons when past performance is not an appropriate evaluation factor for an acquisition. However, the Department has taken the initiative to expand the collection and use of past performance information for competitive solicitations for supplies using FAR part 13 simplified acquisition procedures, including acquisitions valued at less than or equal to $1 million through our Past Performance Information Retrieval System, Statistical Reporting Next Generation (PPIRS-SRNG) system. In order to continue the positive trends achieved to date, DPAP will continue to track and share past performance quarterly results with the Components.

Through 2016, Quarterly Business Senior Integration Group meetings continued with senior leader focus and attention on competition achievement to increase visibility and accountability. At these meetings, the Service Acquisition Executives attributed difficulties with achieving Service goals for competition rates to high value sole source foreign military sales and "Bridge" contracts that impacted competition achievement. Contracts for major non-competitive shipbuilding and aviation programs driven by historical strategic decisions made years ago continued to influence competition opportunities for the long term. In FY 2016, DoD achieved a competition rate of 52.8 percent against a 57 percent goal. In FY 2017, competition will continue to remain a focus item at quarterly Business Senior Integration meetings.

DPAP Conducted Training

On April 27, 2016, DPAP presented two breakout sessions on the subject of competition at the Defense Acquisition University's (DAU) 2016 Acquisition Training Symposium. The Deputy

Director of Contract Policy and International Contracting began each session with an overview of DoD competition policy and statistics. Then Component Program Offices and Contracting Leaders gave presentations highlighting the acquisitions, programs, policies and/or initiative that enabled improved competition and reduced barriers to competition.

On July 19-21, 2016, the Director, Defense Pricing and the Director, Cost Assessment and Program Evaluation hosted the first DoD Contracting and Cost Community Collaboration Conference. This three day event was designed to foster a better reciprocal understanding of pricing and costing estimating capabilities across DoD and to ensure the people on the contract negotiations "front lines" are postured to get the very best deal they can on behalf of the taxpayers using consistent negotiating, estimating and pricing techniques. The approximately 450 attendees were current and future major program lead contracting officers from the Components and DoD cost estimating community.

Improve Tradecraft in Acquisition of Services

On January 5, 2016, DoD released the DoD Instruction (DoDI) 5000.74 - Defense Acquisition of Services. This new instruction establishes policy, assigns responsibilities, and provides direction for the acquisition of contracted services, and implements a management structure for the acquisition of contracted services. This instruction is available at: ***http://www.dtic.mil/whs/directives***.

Over FY 2016, DoD completed full initial implementation of Services Requirements Review Boards (SRRBs) by executing the 4th Estate SRRBs, validating services requirements and joining the Military Departments (MILDEPS) in addressing this statutory requirement. MILDEP and 4th Estate organizations now have processes by which to not only validate requirements, but also to make trade-off decisions regarding competing mission requirements.

Acquisition of Services Functional Integrated Product Team (FIPT) continues the development, execution, and tracking of focused goals, training curriculum, and metrics. The FIPT team has established criteria for identifying the non-Defense Acquisition Workforce Improvement Act (DAWIA) workforce with acquisition-related responsibilities, defined the competencies needed, and identified several training sources for the variety of competencies and skills required for robust services acquisition and management. During FY 2016, the FIPT has identified gaps in training coverage for Functional Services Managers and has developed additional training curricula. Specifically:

- Facilitated two services acquisition (SA) training events for Senior to Mid-Level SA professionals in both the Requirements and Contracting fields. 170 personnel were trained via panel discussion, case studies and exercises, focusing on the roles in SA, BBP, Oversight / DoDI 5000.74, Functional Domain Experts, other SA training initiatives, and SRRBs.
- In June 2016, DAU released the new ACQ 165 Defense Acquisition of Services course and started development of ACQ 255, Program Management for Services Acquisition. Additional training sessions were offered through special sessions of DAU's ACQ 265, Mission Focused Services Acquisition, and COR 222, Training for Contracting Officer Representatives, for non-DAWIA services community stakeholders.
- Army Logistics University in Fort Lee, VA, held 14 additional 10-day Operational Contract Support (OCS) courses in planning, managing, and administering contract service requirements for both Army and other DoD personnel. This existing initiative provided

training for 350 non-acquisition workforce attendees in all facets of OCS, including robust requirements development.

Contracting Officer Representatives

The Department continues to take steps and improve on existing initiatives to improve the effectiveness of contract oversight. The Department published DoDI 5000.72, Department of Defense Standard for Contracting Officer Representative Certification. In addition to explaining the COR nomination and designation process, this instruction identifies the training and experience a COR must fulfill depending on the complexity of the contract action. The instruction also provides a comprehensive list of the potential duties and responsibilities a COR may be delegated by the contracting officer depending on the contract action. The result is to make COR Letters of Designation more specific and complete. The Department continues to analyze COR related training curriculum provided to DoD personnel to make sure it is current and meets learning objectives. DAU has continued to increase the number of Service Acquisition Workshops conducted. DAU also opened up ACQ 265 Mission-Focused Services Acquisition classroom offerings to personnel not in the defense acquisition workforce. These learning assets improve the ability of the workforce, and the development of performance work statements and quality assurance surveillance plans.

The Department is currently developing a COR Guide to streamline the way CORs can learn more about how to execute COR duties, tasks and responsibilities. In addition, the guide will highlight the unique aspects of supply, services, construction, and contingency environment contracts. The guide is intended to be reader friendly and provide better context for the COR.

DAU's contracting training resources continue to focus on COR training. Specifically, DAU's COR Training for FY 2013, FY 2014, FY 2015, and FY 2016 reflect the following number of graduates:

Course Number(s)	Course Name	Graduates FY13	Graduates FY14	Graduates FY15	Graduates FY16*
CLC 106	COR with a Mission Focus	27,892	26,454	26,180	25,974
COR/CLC 206	COR in a Contingency Environment	11,131	7,996	7,410	7,403
COR/CLC 222	Contracting Officer Representative Course	26,341	23,758	26,604	28,114
Total		**65,364**	**58,208**	**60,194**	**61,491**
				* FY16 Total (as of 4 Oct 2016)	
Of note, CLCs 222 and 106 are ranked number five and number six amongst the "most taken" DAU online learning resources.					

The DoD COR Tracking tool, a web-based tool, enables MILDEPS and Defense Agencies to manage nomination, designation, training and tracking of their respective cadres of CORs and the contract(s) assigned to each COR. As of October 2016, there are 63,982 registered CORs.

Buy American Act and Berry Amendment

The Department is currently taking steps to address the Buy American Act and Berry Amendment issues and correct the deficiencies identified in the DoD IG reports, including thoroughly investigating possible cases where the Anti-Deficiency Act may have been violated. The Department is also revising the training curriculum provided to DoD acquisition personnel for both the Buy American Act and Berry Amendment and will require that the new training be taken by DoD contracting personnel in the future. The Berry Amendment continuous learning module,

CLC 125 Berry Amendment, offered by DAU, was updated and made available to the acquisition workforce on September 14, 2016. The Buy American Act revised training (CLC 027) is still in development with an anticipated completion date of April 2017. Once the training packages are fully updated and available to the workforce, the Director of DPAP will prepare guidance to the Defense contracting workforce to require training in these areas. Anticipate guidance issuance in the 3rd quarter of FY 2017.

Illegal Technology Transfer

The Department is committed to maintaining U.S. technical superiority. While we know we are at risk, we are putting mitigation techniques in place to make improvements in areas that may require additional attention. The mitigations include building strategic relationships with our intelligence, counterintelligence and law enforcement government partners to focus resources on protecting sensitive technologies. Through these strategic relationships we are integrating acquisition and technical expertise with expertise from Director of National Intelligence, USD (Intelligence), and Defense Security Service to smartly prioritize our resources on protection of U.S. sensitive technologies.

4 – Increasing Cyber Security and Cyber Capabilities

Offensive and Defense Operations
Technology Platforms and Infrastructure

The Department acknowledges the DoD IG's assessment of Increasing Cyber Security and Cyber Capabilities.

5 – Improving Financial Management

Financial Auditability
Eliminating Improper Payments

Financial Auditability

In FY 2017, 90 percent of General Fund budgetary resources and 54 percent of Working Capital Fund budgetary resources will be under audit; 43 percent of total assets will also be under audit. In FY 2018, 100 percent of DoD assets are projected to be under audit. The number of organizations and the scope of audits will continue to expand until the Department can begin a full agency-wide financial statement audit, likely the largest, single consolidated audit in the world.

In FY 2017, the U.S. Marine Corps will become the first Military Service to have its full financial statements audited. USACE, as well as six Defense Agencies and funds, is already sustaining positive opinions on its full financial statements. The Defense intelligence agencies began full financial statement audits in FY 2015, and two of the largest Defense Agencies (DISA and DLA)

began full financial statement audits in FY 2016. Many of our service providers are sustaining examinations of their controls and systems that can then be used by their Component customer financial statement auditors, saving time and money.

There are benefits to being under audit. The Department's initial audits are helping to drive change while also giving valuable "real world" audit experience. As a result, DoD financial managers and functional leaders have a better understanding of auditors' expectations and the higher level of consistency, discipline, and rigor that auditors require. Operationally, audits give objective feedback on controls, systems, and processes. Corrective actions result in more complete understanding of where the Department's assets are located, and where the Department's costs are actually accruing. This creates opportunities for resources savings and/or reallocation.

While the Department is making great progress, several risk areas remain. It will be several years before the Department begins to see positive audit opinions emerge, so it is critical that we address priority areas of deficiency. The Department has closed 48 percent of the FY 2015 audit findings. The audits of FY 2016 are showing similar results and reinforce the need to resolve the systemic issues of:

- Reducing manual corrections when compiling financial statements, known as journal vouchers,
- Providing accounting details and audit evidence,
- Valuing our property, and
- Retiring legacy Information Technology (IT) systems and deploying audit-ready IT systems.

These systemic issues are rooted in historical accounting practices that must be brought up to today's accounting standards. System work-arounds and the significant progress the Department has made in other areas are enabling DoD to proceed with current audits. However, the magnitude and pervasiveness of these issues will prevent the Department from obtaining a positive opinion. The DoD must identify and resolve the root causes of these issues to fully realize the Department-wide audit goals and benefits.

To ensure that the Department continues to gain value from the audits, the leadership team is focused on monitoring overall progress of audit and remediation of the associated findings. DoD accomplishes the following:

- Notice of Findings and Recommendations/Corrective Action Plans (CAPs) Monitoring - Fourth Estate reports progress monthly, FIAR monitors remediation progress and validates CAP closure.
- The MILDEPs report status of their CAPs during the FIAR Governance Board meetings as well and the board monitors the progress and elevates lack of progress issues as necessary.
- Critical capabilities every 60days –The Department compiles results and produces scorecard that is briefed to FIAR Committee, FIAR Governance Board, and Deputy Management Action Group.

- Interim Milestone Charts - MILDEPs and material Fourth Estate Entities report interim milestones and projected completion dates of each critical capability every 60 days. The Department compiles results and produces charts that are briefed to the FIAR Committee and FIAR Governance Board.

This oversight drives accountability and provides a forum to elevate and address issues that may hinder remediation efforts in support of audit.

Improper Payments

The Department appreciates DoD IG's recognition of our efforts to accurately identify and report improper payments as well as implement corrective actions to reduce improper payments. The Department's improper payment program consists of six individual programs (i.e., military health benefits, military pay, civilian pay, commercial pay, military retiree and annuitant benefit payments, and travel pay) with total outlays greater than $500 billion each fiscal year. Overall, the Department's improper payment program is fundamentally sound as five of the six programs, which account for approximately 99% of total outlays, consistently report exceptionally low percentages (less than one percent) of improper payments each fiscal year. However, the Department continues to exceed its target percentage for travel pay improper payments.

The primary causes for travel pay improper payments are administrative errors, traveler input errors, and inadequate reviews by approving and certifying officials. The Department acknowledges that corrective actions must be implemented to reduce improper payments in the travel pay program and comply with the Improper Payments Elimination and Recovery Act.

Accordingly, the Chief Financial Officer issued a policy memorandum, "Preventing Travel Pay Improper Payments and Enforcing Recovery" on October 7, 2016. The memorandum designates a Department Senior Accountable Official (SAO) for reducing improper payments, emphasizes the significance of front-end internal controls, requires Components to evaluate their travel training effectiveness, re-establishes travel pay improper payment metrics, and reinforces pecuniary liability for erroneous payments resulting from approving improper payments. In addition, the memorandum included a Travel Pay Improper Payments Remediation Plan, which requires each Component to designate an SAO for improper payments and directs Component SAOs to take specific actions to prevent improper payments.

Moreover, the Department continues to aggressively pursue and recover identified improper payments, and through our auditability efforts, improve our methodology for reviewing and identifying the complete universe of disbursements. All of these actions, coupled with the Department's commitment to full financial statement audit, will increase public confidence in the Department's stewardship of taxpayer dollars as well as further strengthen the improper payment program.

6 – Protecting Key Defense Infrastructure
Installations and Energy
Space
Defense Industrial and Technological Base

Installations and Energy

The Department reviewed the DoD IG's assessment of installations and energy and non-concurs. The assessment appears to be misaligned with the Department's information on military construction, renewable energy, operational energy and the use of energy savings performance contracts. Due to the apparent misalignment, this response focuses on the IG's statement:

> Specifically, a series of audits demonstrated that DoD does not have sufficient programs to ensure that energy savings performance contracts (ESPC) and utility energy services contracts were providing cost savings. In some cases, the DoD spent millions on projects that may not have achieved sufficient energy savings to pay back the utility company's investment as required, or to support payments to the contractor based on estimated guaranteed future annual cost savings.

A specific reference for the audits discussed was not provided in the document; however, DoD has taken steps to improve its process.

In coordination with Department of Energy's (DOE) Federal Energy Management Program (FEMP), FEMP published "M&V Guidelines: Measurement and Verification for Performance-Based Contracts (Version 4.0)" which provides the format for reporting any impacts to estimated savings of a given contract. In addition, contractors were informed the DOE ESPC indefinite delivery/indefinite quantity (IDIQ) requires the use of the new guidelines. A similar effort will be coordinated with the Army's ESPC Multiple Award Task Order Contract. Finally, DoD is currently developing a revised reporting process to improve DoD and its Components oversight of third-party financed projects.

In summary, DoD proactively seeks process improvements in third-party financed project oversight. The Department continues to address any IG concerns and will continue to ensure a process is in place to verify third-party financed projects estimated savings.

Space

The Department reviewed the DoD IG's assessment of space and non-concurs. The language as written does not accurately capture the identified challenges. As it is currently written, the language confuses mission assurance, space control, and assured access; and neglects space situational awareness which is a foundational capability to mission assurance and space control.

Defense Industrial and Technology Base

DoD takes a holistic risk-based approach to prevent infiltration of counterfeit parts and materials into the DoD supply chain. This approach spans the product lifecycle and includes:

- Strengthening procurement processes through rulemaking
- Partnering with industry to develop/adopt counterfeit prevention standards
- Increasing workforce awareness through counterfeit prevention training
- Detecting counterfeit parts and materials through materiel inspection and testing
- Reporting counterfeit occurrences in the Government-Industry Data Exchange Program (GIDEP) and monitoring trends
- Managing obsolescence through total life-cycle system management

We are teamed with our industry partners to support their counterfeit programs. Specific industry engagements include participating in anti-counterfeit working groups led by industry associations such as the Aerospace Industry Association and SAE International; leveraging commercial anti-counterfeiting standards such as AS5553, S6174 and AS6081 as we develop proposed concepts of identifying trustworthy suppliers; and holding Government-Industry Call-To-Action meetings to exchange lessons learned and review technical advice on anti-counterfeit practices.

In 2013, the Department established policy and assigned responsibilities with DoDI 4140.67 to prevent the introduction of counterfeit materiel at any level of the DoD supply chain, including special requirements prescribed by section 818 of Public Law 112-81 related to electronic parts. DoD policy requires DoD Components to report all occurrences of suspect and confirmed counterfeit materiel to DoD criminal investigative organizations, and other DoD law enforcement authorities at the earliest opportunity. In addition, DoD Components must report occurrences of suspect and confirmed counterfeit materiel to deficiency reporting systems and the GIDEP within 60 days. We work with law enforcement on counterfeit investigations, and where appropriate, debar companies and prosecute counterfeiters.

To strengthen the GIDEP even further, the Department will publish a new DoD Instruction on use of GIDEP during the first quarter of FY17 which will include identification of roles and responsibilities for submission of reports and oversight of such submission, the level of evidence needed to report a part as suspect counterfeit in GIDEP, and guidance for when access to GIDEP reports should be restricted to government only.

To broaden the understanding of the counterfeit part challenges to the DoD supply chain, the Department has developed training programs taught at DAU focused on understanding how counterfeit parts and materials enter the supply chain; the vulnerability of certain products and processes within the supply chain; techniques to review and audit suppliers; procedures for accountability; and documentation for ensuring materiel authenticity. Other DOD activities have also implemented training programs such as the Defense Logistics Agency, where over 18,000 personnel annually complete counterfeit parts threat awareness training.

The Department has strengthened its counterfeit parts mitigation capability through a number of initiatives. The Defense Logistics Agency quality checks and applies authentication technology Deoxyribonucleic Acid (DNA) to every microcircuit it procures (over 80,000 annually). The DNA mark enables rapid screening of the microcircuit throughout the supply chain and retrieval of the microcircuit's pedigree information anytime throughout its serviceable life. The capability to identify the pedigree information is invaluable during fraud and quality investigations. Enhancements to DOD's Past Performance Information Retrieval Service - Statistical Reporting (PPIRS-SR) provide contacting specialists the capability to identify high risk suppliers, parts that are at higher risk for counterfeiting and parts that are overpriced before awarding contacts. DARPA's Supply Chain Hardware Integrity for Electronics Defense research and development effort seeks to eliminate counterfeit integrated circuits from the electronics supply chain by making counterfeiting too complex and time-consuming to be cost effective. These are just a few of initiatives the Department has implemented to combat counterfeit parts which are not addressed in the IG's summary.

DFARS to the Federal Acquisition Regulation (FAR) addresses counterfeit risk as well, for example:

1. DFARS case (2012-D055) "Detection and Avoidance of Counterfeit Electronic Parts" implements provisions of both FY12 NDAA §818 and FY13 NDAA §833.

2. FAR case (2013-002) "Expanded Reporting of Non-conforming Items" increases and improves the reporting of non-conforming items (including suspected and confirmed counterfeit) into the GIDEP.

3. FAR case (2012-032), "Higher Level Contract Quality Requirements" provides for increased contract quality standards.

4. FAR case (2014 –D005), "Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation" addresses procurement from trusted suppliers and applies to all contractors of electronic parts.

In summary, the DoD has a holistic risk based approach to address counterfeit parts and materials, not only today but into the future. The Department has addressed all GAO concerns and has a robust process in place that will continue to evolve to address the on-going challenge of combatting counterfeit parts and materials introduction into the DoD supply chain.

7 – Developing Full Spectrum Total Force Capabilities

Structure and Posture of the Force and Building Diverse Capabilities Despite Budget Pressures
Chemical, Biological, Radiological, Nuclear, and Explosives Issues

Structure and Posture of the Force and Building Diverse Capabilities Despite Budget Pressures

The Department acknowledges the DoD IG's assessment.

Chemical, Biological, Radiological, Nuclear, and Explosives Issues

The Department reviewed the DoD IG's assessment of Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) issues. Although the Department concurs with the findings, the recommendations focused on unit level logistics and training and did not indicate any CBRNE acquisition programmatic shortfalls. The Department appreciates visibility over these reports to assess potential issues in the fielding of CBRNE equipment. The issues captured in this IG report were not the result of any Chemical and Biological Defense Program fielding issues but rather unit level logistics and command emphasis issues.

The Department has several ongoing efforts to institutionalize corrective actions for the deficiencies noted in the report including the active review and assessment of its policies and standards related to biosafety and biosecurity for Biological Select Agents and Toxins (BSAT) materials. We are ensuring that the DoD IG's recommendations are carefully considered and appropriately captured in policy revisions and in the development of associated guidance.

The Secretary of the Army was designated by the Deputy Secretary of Defense as the Executive Agent (EA) for the DoD BSAT Biosafety Program in July 2015. That designation was included as a responsibility for the Secretary of the Army in the DoDI 5210.88, Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT), published on January 19, 2016. DoDI 5210.88 specifically states the Secretary of the Army "serves as DoD Executive Agent for the DoD BSAT Biosafety Program with responsibility for the technical review, inspection, and harmonization of biosafety protocols and procedures across DoD laboratories that handle BSAT and tasking authority of all DoD Components for this purpose."

The Army Biosafety Task Force established in July 2015 to comprehensively address the issues identified as a result of the inadvertent shipment of live anthrax also came to the conclusion that biosafety and biosecurity are inextricably linked. The Task Force work highlighted that the separation of these programs creates gaps that make the consistent application and oversight of biosafety and biosecurity policies across the Services and labs difficult.

To make the program more effective and reduce the risk to DoD, the EA authority will be expanded to oversee both the biosafety and biosecurity programs for the Department. USD(AT&L) has been directed to promulgate a DoD Directive outlining the roles and responsibilities of the Army EA.

In addition, the Army EA directed that inspections conducted at BSAT facilities be performed by one joint inspection team rather than by multiple teams from the different Services. A detailed inspection plan is being written which will include training requirements for the team as well as procedures for the conduct of inspections.

8 – Building and Maintaining Force Readiness

Equipment Accountability and Reset
Suicide Prevention
Healthcare - Cost, Fraud, Access to Care
Talent Management, Force of the Future

Equipment Accountability and Reset

The Department acknowledges the DoD IG's assessment.

Suicide Prevention

The Defense Suicide Prevention Office, within the Office of the Assistant Secretary of Defense for Readiness, leads working groups of representatives from the Services, the Office of the Assistant Secretary of Defense for Health Affairs, and other stakeholders for the purpose of ensuring a comprehensive approach to suicide prevention. The September 2015 DoD IG report found eight recommendations for improving suicide prevention efforts. All but one of these recommendations are complete. The remaining recommendation concerns the drafting and publication of a DoDI governing the Defense Suicide Prevention Program. A draft Instruction is currently in coordination, and once published all IG recommendations will be met.

Health Care—*Cost, Fraud, Access to Care*

The Department acknowledges the challenges associated with improving access to care within the environment of increasing demand for, and utilization of, care along with constrained resources. Several initiatives have already been implemented to address this, including expanding the Nurse Advice Line, extending hours at clinics, and improving the referral management process. Other initiatives to expand access via non-traditional forums (e.g., secure messaging and telehealth) are in progress.

As of September 30, 2016, DCIS had 494 open health care cases, versus the 492 noted in the IG Report. DCIS' compounding pharmacy investigations have resulted in over $100 million of recoveries, versus the $90 million noted in the IG Report. Furthermore, Health Affairs disagrees with the following sentence in the IG report: "So far in FY 2016, DCIS' health care fraud cases have resulted in 32 criminal charges, 16 convictions, and over $380 million in recoveries for the Government."

DHA has worked closely with the pharmacy contractor to implement additional controls on compound pharmacy claims. This ongoing program has been extremely effective as evidenced by

the reduction in compound drug spending from $497 million in April 2015, to less than $2 million in May 2016, or a 99.6 percent reduction. This reduction in spending has remained constant since May 2016. For additional perspective, spending in May 2016 was near FY 2008 levels, which was prior to any fraudulent compound activity. The TRICARE Pharmacy compound management program still preserves beneficiary access to safe and effective compound medications through the Prior Authorization process.

After a Secretary of Defense-directed, comprehensive 90-day review of the Military Health System (MHS) that focused on access to care, quality of care, and patient safety, the Secretary of Defense issued a memorandum on October 1, 2014, calling for follow-up on performance measures that were identified as statistical outliers in access, quality of care, and patient safety metrics. Other specified tasks from the Secretary included improving transparency and transforming the MHS into a High Reliability Organization. Many initiatives are complete or underway that focus on improving patient care access, safety, and quality. The DoD IG-planned review will continue to assess and provide important feedback not only on the progress of this work to date but also with respect to future strategy and plans.

Talent Management, Force of the Future

The Department reviewed the DoD IG's assessment of Talent management, force of the future issue. However, the Department is unable to validate the section on Air Force pilot shortages and low morale at this time.

The Department does not agree with the IG's use of the word "revitalize" to characterize the goal of Force of the Future. A more accurate description of this effort would be to attract and retain both military and civilian personnel and to develop top-notch talent management systems and processes. Furthermore, it should be noted that while the second set of Force of the Future reforms did originally include initiatives encouraging public service, those initiatives are not being pursued at this time. Rather, the Department would recommend that the DoD IG assess and report on initiatives that are currently being pursued, which include improving quality of life and parental options for military families.

Finally, the Department believes that the Force of the Future initiatives do not indicate that DoD continues to struggle with recruiting and retaining individuals, as noted in the DoD IG report. Projecting perceived pilot shortages as a Department-wide recruitment and retention challenge mischaracterizes a tactical concern as a strategic one. The Department believes that the Force of the Future initiatives, far from responding to a shortcoming, are instead proactive innovations that reflect the changes in today's technology-driven and interdisciplinary environment. These adaptations will ensure that DoD continues to attract and retain top talent in the future.

9 – Ensuring Ethical Conduct

Accountability and Integrity
Whistleblower Issues
Sexual Assault Prevention and Response

Accountability and Integrity

The Department acknowledges the DoD IG's assessment.

Whistleblower Issues

The Department acknowledges the DoD IG's assessment.

Sexual Assault Prevention and Response

The Department reviewed the DoD IG's assessment of Sexual Assault Prevention and Response. The IG report notes that "the DoD IG has a unit staffed with criminal investigators to oversee the DoD's sexual assault investigations." It is unclear whether this unit refers to the new "Reprisal" team focused solely on sexual assault report-related retaliation/reprisal claims. The report's language suggests that the DoD IG investigates all sexual assaults in the DoD; whereas the military criminal investigative organizations have the lead on this.

10 – Promoting Continuity and Effective Transition Management

The Department agrees with the DoD IG's assessment of Promoting Continuity and Effective Transition Management. The Secretary of Defense, all other senior leaders, and the entire Department take the transition from one administration to another very seriously for many reasons, including those highlighted in the IG report. The Secretary has tasked the Department to ensure the most effective and efficient transition possible. On a government-wide level, DoD planning has benefitted from the Presidential Transitions Improvements Act of 2015 and the Executive Order on Facilitation of a Presidential Transition signed by the President in May 2016. Internal to DoD, the Secretary of Defense initiated formal DoD Transition planning in May 2016 as well, consistent with DoD Directive 5105.76, Transition of Administration Appointees and Other Officials. Since that time, a DoD Transition Senior Steering Group and Transition Assistance Coordinators from each major DoD Component have been meeting regularly to implement transition preparation activities across the Department. Consistent with the Presidential Transitions Improvements Act, the Department is on track to certify by November 1st our preparedness to begin transition activities. The dynamic nature of a Presidential transition is significant in scope and scale of leadership positions potentially impacted, particularly across the Office of the Secretary of Defense (OSD) staff where the majority of the political appointee positions exist. The Secretary, and the Department's senior leadership, have continued to ensure maintenance and currency of distinct succession plans for every Presidentially Appointed, Senate-confirmed position, as well as other senior leadership positions. Further, they've ensured that senior career employees are properly prepared to perform the duties of senior leadership positions, as appropriate, should there be a vacancy during transition.

In rough estimation, approximately 10 percent of the OSD positions are political appointees, 20 percent are military, and nearly 70 percent are career personnel. Therefore, a core cadre remains even in the most dynamic times; and from this the Department works its deliberate transition planning. The Department appreciates the points made by the IG and is firmly committed to a transition that is smoothly carried out in a highly effective and efficient manner.

Naval Facilities Engineering Command, Engineering and Expeditionary Warfare Center managed the deployment of the Fred. Olsen Ltd. "Lifesaver" Wave Energy Conversion device between March 22 and 25, to the Navy's Wave Energy Test Site. NAVFAC EXWC established and still manages the WETS facility located off Marine Corps Base, Hawaii.

U.S. Navy Photo (Released)