

**DFAS Civilians by Site and Grade On Board as of May 16, 2005**

DFAS Location	Total	2	3	4	5	6	7	8	9	10	11	12	13	14	15	SES
ARLINGTON	371			4	3	1	8	8	23		9	29	96	126	51	13
CHARLESTON	360			28	51	64	104	15	18	1	47	22	7	2	1	
CLEVELAND	1184		11	49	93	138	123	26	94	1	175	301	123	36	12	2
CLEVELAND BRATENAHL	10				1							5	4			
COLUMBUS	2040		2	66	262	348	413	41	100	2	253	328	163	48	12	2
DAYTON	350	1	2	14	89	92	69	11	17	1	30	12	9	1	2	
DENVER	1175	2	1	29	62	55	184	46	154	2	156	291	142	38	12	1
INDIANAPOLIS	2479	2	21	87	323	301	348	39	92	2	310	585	263	73	30	3
KANSAS CITY	669			22	29	41	105	7	48	1	157	163	70	17	7	2
LAWTON/FT SILL	268	1		2	102	63	24	16	11		33	9	5	2		
LEXINGTON	39				11	6	6		3		7	4	1	1		
LIMESTONE	352			2	161	82	43	15	6	1	21	14	5	1	1	
NORFOLK	340		8	33	55	95	55	4	23		27	26	11	2	1	
OAKLAND	50				12	8	1		1		19	8	1			
OMAHA	232			2	38	100	24	10	20		22	12	3		1	
ORLANDO	218	1	3	3	50	45	34	13	11		39	14	4	1		
PACIFIC (Ford Island)	180				51	48	21	5	16		23	10	4	1	1	
PATUXENT RIVER	56				1				6			27	18	4		
PENSACOLA	335	1	5	11	72	36	100	19	15		27	26	16	4	3	
PENSACOLA SAUFLEY FIELD	186			1	2	2	2		13		18	110	28	8	2	
RED RIVER ARMY DEPOT (AF only)	56					30	5		9		6	6				
ROCK ISLAND	305	1	2	4	62	63	58	12	16		39	40	4	3	1	
ROME	382	1		5	170	75	49	20	4		38	13	5	1	1	
SAN ANTONIO	314	1	1	9	114	62	55	12	19		25	13	2	1		
SAN BERNARDINO	113		1	1	48	16	10	5	5	1	15	7	3	1		
SAN DIEGO	311	1	5	5	47	114	33	9	12		62	13	9	1		
SEASIDE	47			1	12	7	2	2	3		10	2	6	2		
ST LOUIS	324			6	62	69	71	16	13		43	36	6	1	1	

Library Routing Slip 2005 BRAC Connection Materials

Title of Item: DFAS employees & security assessments

Installation or Community: DFAS

Source: DFAS

Certified Material?  yes  no

Analyst / Provider: J. Claski Date Received: 9/1/05

**FOR OFFICIAL USE ONLY**DFAS COLUMBUS SECURITY ASSESSMENT

- DFAS Columbus is a tenant activity within the Defense Supply Center, Columbus (DSCC), which is located in Columbus, Ohio. DFAS Columbus occupies buildings 11 and 21 with building 21 being the primary DFAS facility.
- As DFAS Columbus is a tenant of DSCC, the Commander, DSCC maintains primary Force Protection responsibility for the installation. As such, DSCC provides physical security, police and guard, fire, medical, and a host of other related services. As DFAS Columbus is a tenant of a DoD installation, the DoD Force Protection Condition System is implemented.
- Access is controlled to the installation by the DSCC security force. Access to building 21 is controlled through the use of an electronic entry control system. Visitors are processed through the main entrance, which contains a visitor pass office and is monitored by a DSCC armed police officer.
- Delivery vehicles are screened by the DSCC security force prior to being granted access to the installation. Incoming mail is screened in the mailroom through the use of x-ray technology.
- Closed Circuit Television (CCTV) is installed on both the interior and exterior of the facility and is monitored by the DSCC security force. The security force also conducts patrol activity on both the interior and exterior of the facility.
- The HVAC systems for building 21 are located in several mechanical rooms throughout the building with air intake and exhaust vents located on the roof. Building 21A does have HVAC vents at ground level but perimeter fencing protects them. Building 11 have HVAC vents at ground level that pose potential vulnerabilities. Potable water is supplied by local public utilities using an underground feed.
- DFAS last conducted an assessment (Executive Summary attached) at the DFAS Columbus site in April 2003. At that point in time the threat was assessed at Low. A comprehensive Higher Headquarters Vulnerability Assessment utilizing the Joint Staff Integrated Vulnerability Assessment (JSIVA) methodology and benchmarks, to include application of standards contained in Unified Facilities Criteria (UFC) 4-010-01 (DoD Minimum Antiterrorism Standards For Buildings) is being scheduled for late FY 2005.
- Major physical security concerns identified in the April 2003 assessment included standoff, HVAC emergency shut off switches, and other administrative issues. Measures taken to mitigate identified concerns include installation of fragmentation retention film, bollards and barriers, an HVAC cutoff switch in the mailroom, and a new electronic entry control system.

Attachment:

As stated

Prepared by: Hugh D. Wiley, (317) 510-4096

**FOR OFFICIAL USE ONLY**



---

# **Safety, Protection, Infrastructure, Recovery Integration Team (SPIRIT)**

---

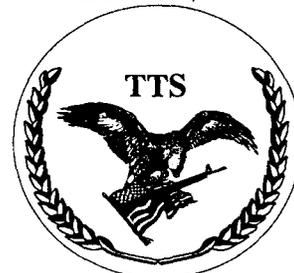
## **Summary Report for Defense Finance and Accounting Service (DFAS) – Columbus, Ohio**

**Assessment Period: April 7 to 11, 2003**

### **FOR OFFICIAL USE ONLY**

**This document contains information exempt from mandatory  
disclosure under the FOIA. Exemptions 2 and 5 apply.**

TACTICAL TRAINING  
SPECIALISTS, LLC



"PROFESSIONAL DEVELOPMENT  
THROUGH  
ADVANCED TRAINING"

---

**PRODUCED FOR DEFENSE FINANCE AND ACCOUNTING SERVICE BY  
TACTICAL TRAINING SPECIALISTS, LLC UNDER CONTRACT #MDA210-02-P-0006**

---

**FOR OFFICIAL USE ONLY****DFAS – Columbus Center****I. EXECUTIVE SUMMARY****A. INTRODUCTION**

In May 1998, President Clinton issued two Presidential Decision Directives, PDD-62, Combating Terrorism, and PDD-63, Critical Infrastructure Protection. The two PDDs assign responsibilities and actions associated with national level critical infrastructure protection, including physical and cyber-based systems essential to the minimum operations of the government and economy. The many terrorist attacks to the United States and its allies, culminating on September 11, 2001 at the World Trade Center Towers and the Department of Defense's Pentagon, resulted in President Bush issuing Executive Orders 13228 and 13231. The Orders require all government agencies to identify critical infrastructure elements, assess potential vulnerabilities, and implement measures to protect those critical elements.

The Defense Finance and Accounting Service (DFAS) Headquarters reviewed the collective requirements of the two PDDs and the two Executive Orders. Particular attention was addressed to Executive Order 13228's requirement for the heads of all agencies to "ensure the health and security" of their employees. DFAS responded to these requirements by identifying the key programs necessary to achieve the safety and security of its work force and infrastructure. The combination of the key programs resulted in the Safety, Protection, Infrastructure, and Recovery Integration Team (SPIRIT) concept. SPIRIT incorporates the following programs; Safety and Occupational Health, Personnel Security, Information Security, Physical Security and Anti-Terrorism / Force Protection, Contingency Planning, Information Assurance, and Critical Infrastructure Protection.

## FOR OFFICIAL USE ONLY

The mission objectives of SPIRIT incorporate a combined strategy. First, SPIRIT will benchmark the agency wide implementation and directive compliance for each program. During this process, SPIRIT will also identify the key infrastructure elements and the policy, procedures, and methods presently utilized to protect the key elements. Based upon this identification and benchmarking, SPIRIT will analyze the program results and offer recommendations for program improvement and vulnerability mitigation. Lastly, the SPIRIT strategy assumes the strong implementation of each of the SPIRIT programs, must be integrated, to achieve protection of DFAS personnel, systems, and infrastructure. Program integration will be analyzed and improved by introducing training and exercises targeted to test the agency's contingency plans and readiness. The combined strategy's objective is to meet the requirements of the PDDs and Executive Orders, and ensure the protection of the DFAS infrastructure and critical elements.

### B. SPIRIT VISIT DATES AND TEAM ASSIGNMENTS

The SPIRIT Assessment was conducted April 7 to 11, 2003 at DFAS- Columbus (DFAS-CO). The following personnel participated in assessment:

#### **DFAS Program Managers:**

Mr. Marvin Lewis	DFAS Physical, Personnel Security, Information Security, Physical Security and Anti-Terrorism/Force Protection
Ms. Kim Ponder	Information Assurance (IA)
Ms. Dianne Ferrante	Critical Infrastructure Protection

#### **Tactical Training Specialists, LLC (TTS) Assessment Team:**

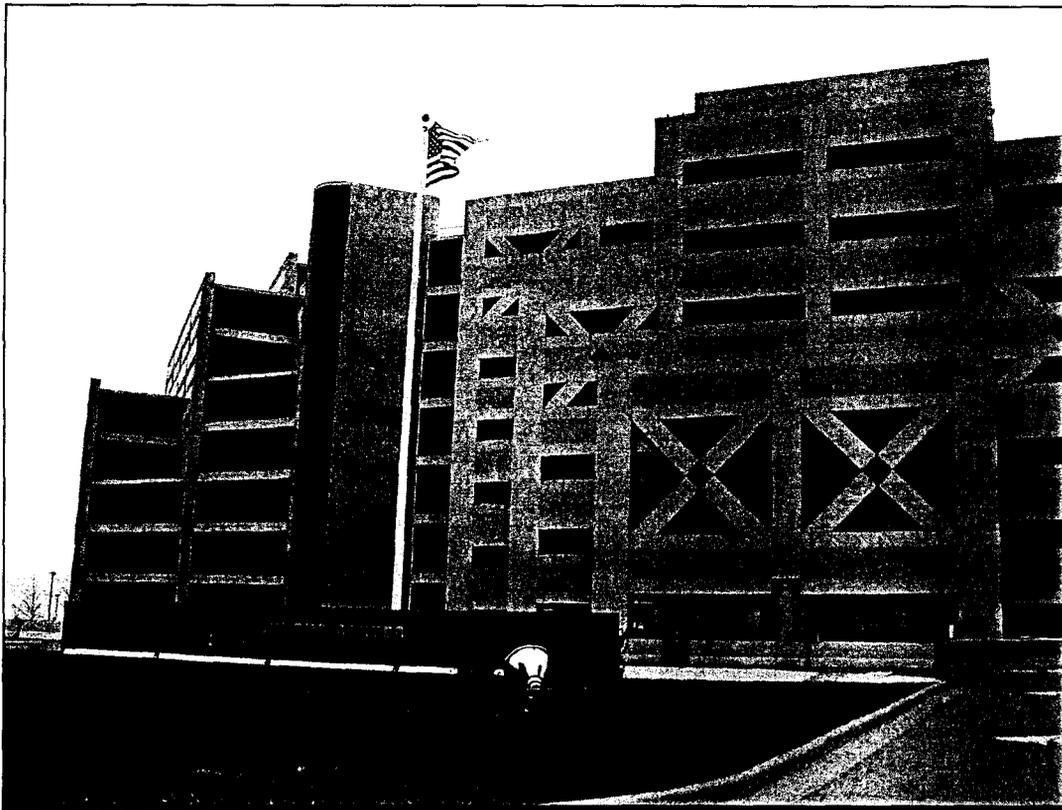
Randal Justus	TTS Team Lead, Personnel Security, Information Security, Physical Security, and Contingency Planning Programs
Wendy Johnson	Safety and Occupational Health Programs
Fredric Borchardt	Physical Security, Antiterrorism/Force Protections
Daniel Stocking	Physical Security, Antiterrorism/Force Protection
Jose Torres	Physical Security, Antiterrorism/Force Protection
Charles Butler, Ph.D.	IA and CIP
Maryfrances Herrera	IA and CIP

**FOR OFFICIAL USE ONLY****C. DFAS- COLUMBUS SITE DESCRIPTION AND BACKGROUND**

DFAS - Columbus (DFAS-CO) is a tenant activity within the Defense Supply Center, Columbus (DSCC), located in the southeast quadrant of the City of Columbus (see the Columbus Vicinity Map at Attachment A). The majority of 2,079 DFAS-CO federal and contractor personnel are located in Building 21. This is a very modern, high-rise building, which was completed in 1999 and occupied by DFAS in 2002. DFAS personnel also occupy buildings 10 and 11, which are much older DSCC buildings (see the DSCC map at Attachment B).

DFAS-CO benefits by the many services provided by the host. Inclusive in the services provided are physical security systems, police and guard service, fire department, medical services, facilities maintenance, personnel security support, emergency operations command and control, utilities, vehicle and personnel badge and pass functions, and connectivity to the Defense Enterprise Computing Center (DECC).

DFAS-CO business or product lines are Accounting and Travel Pay Services. The Accounting Business Line processes 52,094 general ledger accounts requiring over 95,400,000 manual and automated journal entry lines per year. Travel Pay Services compute and process Temporary Duty (TDY) and Permanent Change of Station (PCS) travel vouchers (or entitlements) for military and civilian employees traveling on customer funds. Columbus processes an average of 21,000 vouchers, resulting in \$14,500,00 in disbursements per month. A listing of DFAS-CO's customers is provided (see Attachment C).

**FOR OFFICIAL USE ONLY**

*Building 21*

**D. SAFETY AND OCCUPATIONAL HEALTH PROGRAMS**

The assessment was conducted by comparison of the Site's SOH Program implementation with the requirements of DoD regulations and instructions, the Occupational Safety and Health Administration Regulations, and other directives listed as references in the SOH Site report. Regulatory program documentation and reports were reviewed. Walkthroughs of facilities and grounds were performed, and employee surveys and interviews were conducted to determine the Site's commitment to SOH concepts and to identify potential SOH risks.

DFAS-CO has functionally implemented a strong SOH program. The well-implemented ergonomic program conducts weekly evaluations and makes workstation adjustments as necessary. Currently, there are no injuries or illnesses related to ergonomic issues. Other program strengths include quarterly safety inspections, new-hire and periodic safety training, implementation of Building 21 Safety Council, medical services located within the building, and implementation of other SOH programs.

## FOR OFFICIAL USE ONLY

As is the case at many DFAS sites, the program lacks a written, safety and health policy (signed by the senior site manager) as required by DoD Instruction 6055.1. Five other program discrepancies are identified in the SOH Site Report.

### E. PHYSICAL SECURITY, ANTI-TERRORISM / FORCE PROTECTION PROGRAMS

DFAS-CO's Physical Security and Antiterrorism/Force Protection Programs were assessed by comparison of the Site's program implementation with the requirements and standards of DoD Instruction 2000.16, DoD Antiterrorism Standards and DFAS 5200.8-R, DFAS Physical Security Regulation, and best security practices. The Joint Staff Integrated Vulnerability Assessment (JSIVA) survey was utilized to determine the Site's security preparedness versus the DoD 2000.16 standards.

The Site's Security Manager, Security Specialist, police and fire personnel, Facility Manager, and Contingency Planner were interviewed. Site tours, during both working hours and darkness, were conducted to observe security systems and their effectiveness, and identify potential vulnerabilities. The Site's Occupant Emergency Plan and Antiterrorism/Force Protection Plan were reviewed to determine their effectiveness. An evaluation of the Site's ability to implement the Force Protection Levels (ALPHA through DELTA) was performed. Threat assessment reports and other documentation were reviewed to evaluate the threats and probability of attack on the site.

The DSCC Police Department provides first responder police services for this facility. During the time of this assessment the current threat level was at "CHARLIE". Security is augmented by several security systems and capabilities. Several opportunities for improvement were identified in the Physical Security/Antiterrorism/Force Protection report along with other general physical security improvements.

### F. PERSONEL SECURITY PROGRAM

The Personnel Security Program was assessed by comparison of the requirements of DOD 5200.2-R, Personnel Security Program, and DFAS 3020.26R, Corporate Contingency Plan with DFAS – CO's program implementation.

The Personnel Security Program at DFAS – CO is very strongly implemented. The staff that implements and administers the program is well trained and knowledgeable of Personnel Security requirements, and has the complete confidence and cooperation of management. Site personnel have worked together to correctly classify positions of trust and positions requiring classified information access, and to ensure personnel occupying those positions have the appropriate background investigation and periodic reviews requisite for the positions.

## FOR OFFICIAL USE ONLY

DFAS – CO has entered into a service agreement with the DSCC Personnel Security Office. DSCC provides administrative, Personnel Security services for all DFAS – CO federal employees. This support allows the DFAS Personnel Security Specialist to focus on Personnel Security program administration for the many contractor personnel utilized by DFAS – CO. The utilization of DSCC Personnel Security support is efficient, cost effective, and viewed as a best business practice within DFAS.

### G. INFORMATION SECURITY PROGRAM

The Information Security Program was evaluated by comparison of DOD 5200.1-R, Information Security Program, requirements, with the program implementation at DFAS-Columbus. The Program has been implemented satisfactorily and complies with directives to protect the large amounts of classified material stored and utilized at the site. Considerable classified material is utilized, stored, and protected as a result of a special Contract Pay mission. This is in addition to the classified and sensitive material produced and held in the Emergency Operations Center (EOC).

Given the magnitude of classified material held, the size and complexity of the security requirements imposed by location and tenant relationship, and the various programs/personnel accessing classified information, it is recommended that a site Security Manager be designated. The Security Manager should be responsible for integrating all the security programs to ensure the protection of personnel, facilities, and classified matter; and to ensure full requirements with all security regulations. Other minor opportunities for improvement were identified, and are included in the Information Security Report.

The Information Security Assessment performed at DFAS-Columbus meets the DOD 5200.1R requirement for annual, Information Security assessments of subordinate units by higher authority.

### H. CONTINGENCY PLANNING /CONTINUITY OF OPERATIONS

The Contingency Planning Program was assessed utilizing the standards and requirements of DFAS 3020.26-R, Corporate Contingency Plan. The DFAS-Columbus contingency planning program is compliant, with current plans entered into the Living Disaster Recovery Planning System (LDRPS). Emergency, Alternate Processing, Relocation, and Continuity of Operations plans are being reviewed annually.

DFAS – CO has the second largest contingency planning staff of all DFAS sites. In addition to normal contingency plans, the DFAS – CO planners develop generic plans for the agency. The generic plans have standardized contingency plans for the DFAS, have eliminated redundancy, and have raised efficiency in the Agency's contingency planning effort.

## FOR OFFICIAL USE ONLY

A member of the DFAS – CO contingency planning staff is the Agency's sole scheduler and coordinator for information systems testing for mission critical systems operated at Defense Enterprise Computing Center (DECC) sites. This individual establishes the requirements for continuity of operations plans (COOP) and testing of the DFAS systems at the DECCs. He schedules the tests, accepts the test plans developed by the DECCs, evaluates the test results, and ensures after action reports are forwarded. This effort is critical to the Agency's COOP ability, but is also imperative to the accreditation of DFAS information systems. Due to the critical nature of this activity, additional personnel should be assigned and trained to perform these duties, for contingency purposes. Other program strengths and opportunities for improvement are identified in the Contingency Planning DFAS – Columbus Report.

### I. INFORMATION ASSURANCE (IA)

The objectives of the Information Assurance (IA) assessment were to review DFAS Columbus's implementation of DFAS Regulation 8000.1-R, DFAS Information Management Program Policy, Part G. Information Assurance Policy, requirements, evaluate compliance, and make recommendations for improvement. As DFAS-CO is a center and manages systems for the DFAS Agency, an additional objective was to determine the status of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) certification and accreditation packages for six mission essential systems.

DFAS-CO exhibited a strong implementation of the IA policies. Information systems security personnel were knowledgeable concerning their IA duties and responsibilities. Workstation and password lockout compliance adheres to the DFAS policies, as observed during walkthrough visits of the work areas. Additionally, web access is monitored through the use of systems software.

Opportunities for improvement generally involved the need to increase awareness and site personnel knowledge concerning the identify of the Information Systems Security Manager, systems accreditation and certification status, System Security Authorization Agreement status, and the Systems Inventory Database.

A significant Agency vulnerability exists in that five of six mission essential systems do not have DITSCAP accreditation or Authorization to Operate (ATO). The one system with an ATO (Defense Business Management System or DFMS) has the authorization expiring on October 31, 2003. Strategies for accrediting the five deficient systems were recommended.

**FOR OFFICIAL USE ONLY****DFAS-CO Systems**

<b>System Name</b>	<b>System Acronym</b>	<b>System Priority</b>	<b>Accreditation Status</b>
1099	1099	Mission Essential	Interim ATO is expired
Contract Reconciliation System	CRS	Mission Essential	No ATO. Submit for Interim ATO
Defense Business Management System	DBMS	Mission Essential	ATO is current.
Defense Disbursing Analysis Reporting System	DDARS	Mission Essential	No ATO. Submit for Interim ATO
Entitlements Automation System	EAS	Mission Essential	Expired ATO. Resubmit
Prevalidation Management Information Reporting System	PMIRS	Mission Essential	Submit for ATO

**J. CRITICAL INFRASTRUCTURE PROTECTION (CIP)**

The objectives of the CIP assessment were based upon PDD-63, Critical Infrastructure Protection and DFAS 3020.26-R, Corporate Contingency Plan. Assessment objectives were to:

1. Identify information system vulnerabilities and risks.
2. Identify a significant, single point of vulnerability.
3. Evaluate business continuity plans for contingency recovery.

CIP objectives were reviewed in conjunction with business continuity and reconstitution requirements for center site personnel using mission essential systems. Reconstitution capabilities for other systems were also discussed.

Several CIP strengths were noted. The Assistant Information Systems Security Manager promotes contingency plans for mission essential and other systems. Individual systems recovery plans are near completion. Secondly, two mission essential systems have been tested for recoverability (DBMS and EAS). Thirdly, the site is aware and attempts to manage and inventory site developed, Access Program applications developed by other than Technical Services Organization personnel. Nearly 3, 000 such applications exist at the site.

## FOR OFFICIAL USE ONLY

Opportunities for improvement included recommendations to exercise the recoverability of backup data, increasing site personnel's knowledge and awareness of contingency plans, the need to review memorandum of understanding agreements for alternate site processing, and the development of contingency plans for the e-Biz system.

### K. CLOSING REMARKS

DFAS-Columbus program management personnel were professional, candid, and cooperative. Columbus was well prepared for the SPIRIT visit and had all documentation available. The SPIRIT members thank DFAS-Columbus for hosting the visit, and for the hospitality extended to the Team.

Each of the report sections identifies programmatic strengths, as well as opportunities for improvement, if warranted. No grades are assigned to the programs. As stated, the SPIRIT mission objective is to benchmark the Agency wide implementation of the programs comprising SPIRIT.

Please forward all comments regarding this report to Mr. Ed Kufeldt at DFAS Headquarters, Arlington, Virginia. ED.KUFELDT@DFAS.MIL

#### **Attachments:**

- a. Columbus Vicinity Map
- b. Defense Supply Center, Columbus (DSCC) Map
- c. DFAS-CO Customer List



**FOR OFFICIAL USE ONLY**DFAS DENVER SECURITY ASSESSMENT

- DFAS Denver is a tenant activity of Buckley Air Force Base, which is located within metropolitan Denver, Colorado. DFAS Denver occupies buildings 407, 409, and 444 with building 444 being the primary DFAS facility.
- As DFAS Denver is a tenant of a DoD installation, the Commander, Buckley Air Force Base maintains primary Force Protection responsibility for the installation. As such, Buckley Air Force Base provides physical security, police and guard, and other related services. As a tenant of a DoD installation, the DoD Force Protection Condition System is implemented.
- Access is controlled to the installation by armed contract security forces. Access is controlled to the DFAS building through the combination of security personnel and electronic entry control systems. Screening equipment is available to assist in access control duties. Visitors are required to be escorted while in the DFAS Denver complex. A vehicle resistant barrier (bollard and cable system) that encompasses building 444 supports over 100 feet of standoff.
- Delivery vehicles are screened by security personnel prior to being granted access to the installation and again upon arrival at building 444. Incoming mail is screened and opened in the mailroom. Mail is screened through the use of x-ray technology and all mail is opened electronically through the use of a mail opening system that opens mail in front of a exhaust system equipped with a High Efficiency Particulate Air (HEPA) filtration system.
- Closed Circuit Television (CCTV) and Intrusion Detection Systems are installed throughout the DFAS Denver complex and monitored by the on-site security force. The security force also conducts patrol activity on both the interior and exterior of the facility.
- The HVAC systems are located both on the roof and at ground level. Those located at ground level represent a potential vulnerability. Water is supplied by local public utilities using underground feeds.
- DFAS last conducted an assessment (Executive Summary attached) at the DFAS Denver site in November 2002. At that point in time the threat was assessed at Low to Medium dependant on tactic assessed. A comprehensive Higher Headquarters Vulnerability Assessment utilizing the Joint Staff Integrated Vulnerability Assessment (JSIVA) methodology and benchmarks, to include application of standards contained in Unified Facilities Criteria (UFC) 4-010-01 (DoD Minimum Antiterrorism Standards For Buildings) is being scheduled for late FY 2005.

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

- Major physical security concerns identified in the November 2002 assessment included standoff, HVAC emergency shut off switches, fencing, CCTV system upgrades, and lighting. Measures taken to mitigate identified concerns include installation of fragmentation retention film, additional barriers, an HVAC cutoff switch in the mailroom, and an upgrade to the electronic security system.

Attachment:

As stated

Prepared by: Hugh D. Wiley, (317) 510-4096.



---

# **Safety, Protection, Infrastructure, Recovery Integration Team (SPIRIT)**

---

## **Summary Report for Defense Finance and Accounting Service (DFAS) –Denver (DFAS-DE)**

### **FOR OFFICIAL USE ONLY**

This document contains information exempt from mandatory disclosure under the FOIA. Exemptions 2 and 5 apply.

TACTICAL TRAINING  
SPECIALISTS, LLC



"PROFESSIONAL DEVELOPMENT  
THROUGH  
ADVANCED TRAINING"

---

**PRODUCED FOR DEFENSE FINANCE AND ACCOUNTING SERVICE BY  
TACTICAL TRAINING SPECIALISTS, LLC UNDER CONTRACT #MDA210-02-P-0006**

---

**FOR OFFICIAL USE ONLY****DFAS – Denver Field Site****I. EXECUTIVE SUMMARY****A. INTRODUCTION**

In May 1998, President Clinton issued two Presidential Decision Directives, PDD-62, Combating Terrorism, and PDD-63, Critical Infrastructure Protection. The two PDDs assign responsibilities and actions associated with national level critical infrastructure protection, including physical and cyber-based systems essential to the minimum operations of the government and economy. The many terrorist attacks to the United States and its allies, culminating on September 11, 2001 at the World Trade Center Towers and the Department of Defense's Pentagon, resulted in President Bush issuing Executive Orders 13228 and 13231. The Orders require all government agencies to identify critical infrastructure elements, assess potential vulnerabilities, and implement measures to protect those critical elements.

The Defense Finance and Accounting Service (DFAS) Headquarters reviewed the collective requirements of the two PDDs and the two Executive Orders. Particular attention was addressed to Executive Order 13228's requirement for the heads of all agencies to "ensure the health and security" of their employees. DFAS responded to these requirements by identifying the key programs necessary to achieve the safety and security of its work force and infrastructure. The combination of the key programs resulted in the Safety, Protection, Infrastructure, and Recovery Integration Team (SPIRIT) concept. SPIRIT incorporates the following programs; Safety and Occupational Health, Personnel Security, Information Security, Physical Security and Antiterrorism / Force Protection, Contingency Planning, Information Assurance, and Critical Infrastructure Protection.

## FOR OFFICIAL USE ONLY

The mission objectives of SPIRIT incorporate a combined strategy. First, SPIRIT will benchmark the agency wide implementation and directive compliance for each program. During this process, SPIRIT will also identify the key infrastructure elements and the policy, procedures, and methods presently utilized to protect the key elements. Based upon this identification and benchmarking, SPIRIT will analyze the program results and offer recommendations for program improvement and vulnerability mitigation. Lastly, the SPIRIT strategy assumes the strong implementation of each of the SPIRIT programs, must be integrated, to achieve the protection of DFAS personnel, systems, and infrastructure. Program integration will be analyzed and improved by introducing training and exercises targeted to test the agency's contingency plans and readiness. The combined strategy's objective is to meet the requirements of the PDDs and Executive Orders, and ensure the protection of the DFAS infrastructure and critical elements.

### B. SPIRIT VISIT DATES AND TEAM ASSIGNMENTS

The SPIRIT Assessment was conducted November 12 – 22, 2002 at DFAS- DENVER (DFAS-DE). The following personnel conducted the SPIRIT Assessment:

#### **DFAS Program Managers:**

Mr. Marvin Lewis	Personnel Security, Information Security, Physical Security, and Antiterrorism / Force Protection Programs
Ms. Codie Smith	Information Assurance (IA) and Critical Infrastructure Protection (CIP)
LCOL Marie Rigotti	Information Assurance

#### **Tactical Training Specialists, LLC (TTS) Assessment Team:**

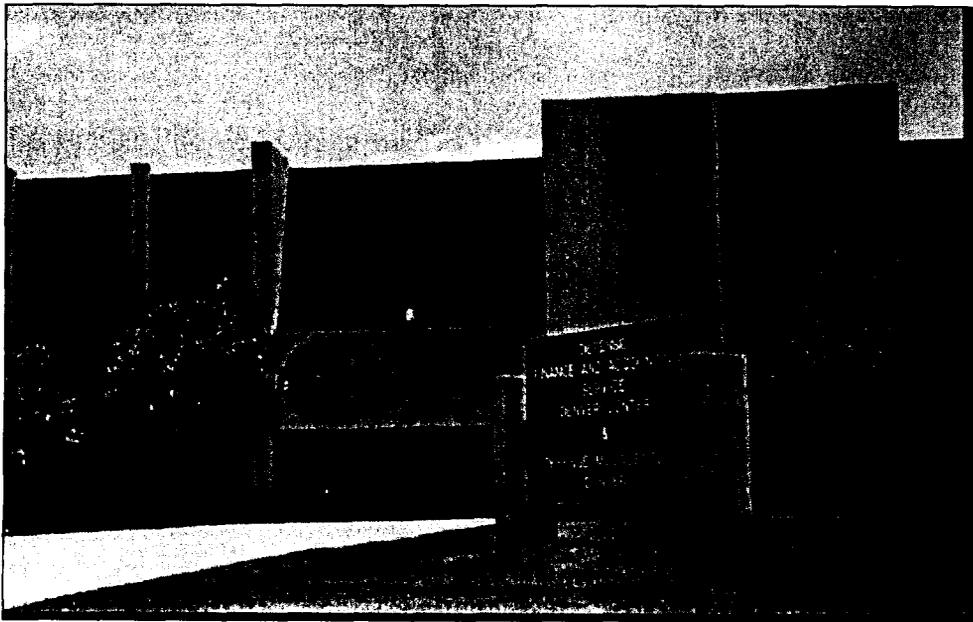
Randal Justus	Tactical Training Specialists LLC (TTS) Team Lead, Personnel Security, Information Security, and Contingency Planning Programs
Rick Shassetz	Safety and Occupational Health Programs
Joann Jackson-Bass	Safety and Occupational Health Programs
Bret Aduddell	Physical Security, Antiterrorism/ Force Protection
Dan Stocking	Physical Security, Antiterrorism / Force Protection
Van Hall	Physical Security, Antiterrorism / Force Protection
Charles Butler, Ph.D.	Information Assurance and Critical Infrastructure Protection

## FOR OFFICIAL USE ONLY

### C. DFAS DENVER SITE DESCRIPTION AND BACKGROUND

The Defense Finance and Accounting Service – Denver (DFAS-DE) is located on the former Lowry Air Force Base and was activated on January 18, 1991. Director Zack Gaddy oversees the efforts of the site's 1,800 personnel and is responsible for oversight of a network of five field sites (Dayton, Limestone, Omaha, San Antonio, and San Bernardino).

The Denver facility is located on 78 acres of land within the city limits of Denver, in the southeast quadrant. The current population is approximately 2,450 military, civilian and contractors working in five buildings. The main DFAS facility (Building 4444) was constructed in July 1976. The Air Force Accounting and Finance Center was one of the first tenants to move into the 605,500 square foot facility. Other tenants include the Air Reserve Personnel Center (ARPC), with approximately 1,700 to 1,800 personnel, the Space Age Credit Union (SACU), and the Defense Enterprise Computing Center (DECC)-Denver. An aerial view of the DFAS-DE site is included at Attachment A to this section.



*Main Entrance to Building 444*

DFAS-DE manages, administers, and/or operates nineteen mission critical or mission essential systems. The site manages and performs operations within the following business/product lines:

1. Military and Civilian Pay
2. Vendor Pay
3. Accounting and Finance
4. Disbursing (to include check production)

## FOR OFFICIAL USE ONLY

DFAS-Denver primarily services the Air Force, DoD Security Assistance Program (Foreign Military sales), and other select DoD agencies.

### D. SAFETY AND OCCUPATIONAL HEALTH PROGRAMS (SOH):

The assessment was conducted by comparison of the Site's SOH Program implementation with the requirements of DoD regulations and instructions, the Occupational Safety and Health Administration Regulations, and other directives listed as references in the SOH Site report. Regulatory program documentation and reports were reviewed. Walkthroughs of facilities and grounds were performed, and employee surveys and interviews were conducted to determine the Site's commitment to SOH concepts and to identify potential SOH risks.

The SOH programs were determined to be fully implemented, well documented, and highly effective. The Site SOH Manager has appointed and trained safety monitors who assist in conducting regular safety inspections. Employees receive SOH indoctrination, ergonomic, and refresher SOH training. The safety survey indicated employees are knowledgeable concerning SOH programs and avenues that can be utilized to correct concerns.

The program implementation has been highly successful. Since 1996, the total reportable mishaps have reduced from 189 to 76 (63% reduction). The ergonomic program has conducted over a 1,000-workstation intervention and has benefited by an 80% decrease in ergonomic injuries in the same period.

Other site strengths include:

1. Denver has the preeminent mailroom exhaust system for potential hazard control during mail opening operations, in the DFAS agency. By mandate, all mail received at the site is opened in the mailroom and within the protection of the exhaust system. The mailroom area also contains a shower facility that has been modified to become a personnel decontamination facility that captures and contains runoff water and contaminants.
2. The Safety Management Council meets regularly to discuss current safety issues.
3. A Federal Occupational Health Clinic, staffed by two nurses with physician access, operates within Building 444.
4. Indoor air quality (IAQ) investigations have been conducted to address employee concerns.
5. Realistic emergency drills are conducted and interviewed employees were knowledgeable concerning their responsibilities and escape routes, should an emergency occur.

## FOR OFFICIAL USE ONLY

### Opportunities for improvement included:

1. Review of the site's five years safety inspection reports revealed some repeat findings had not been mitigated from one year to the next.
2. Safety goals should be included and evaluated for achievement in both employee and management performance appraisals.
3. A joint safety committee should be established with the other tenants in the DFAS-DE occupied buildings.
4. Many ladders were observed, around the site, which were not stored/secured properly. A formal, ladder safety program should be developed which includes storage, use, and inspection of ladders.
5. Numerous electrical safety issues were identified in the Maintenance Building (Building 409), which should be corrected.
6. Consideration should be given to eliminating the respirators in the Mailroom due to the in-place exhaust system. Eliminating the respirators eliminates the need for a Respiratory Protection Program.
7. The safety issues identified during the walkthrough of Building 667 (DFAS warehouse and Lowry Teen Center) should be mitigated.

### E. PHYSICAL SECURITY, ANTITERRORISM / FORCE PROTECTION PROGRAMS

DFAS - Denver's Physical Security and Antiterrorism/Force Protection Programs were assessed by comparison of the Site's program implementation with the requirements and standards of DoD Instruction 2000.16, DoD Antiterrorism Standards and DFAS 5200.8-R, DFAS Physical Security Regulation, and best security practices. The Joint Staff Integrated Vulnerability Assessment (JSIVA) survey was utilized to determine the Site's security preparedness versus the DoD 2000.16 standards.

The Site's Security Specialist, guard personnel, Facility Manager, and Contingency Planner were interviewed. Site tours, during both working hours and darkness, were conducted to observe security systems and their effectiveness, and identify potential vulnerabilities. The Site's Occupant Emergency Plan and Antiterrorism/Force Protection Plan were reviewed to determine their effectiveness. An evaluation of the Site's ability to implement the Force Protection Levels (ALPHA through DELTA) was performed. Threat assessment reports and other documentation were reviewed to evaluate the threats and probability of attack on the site.

## FOR OFFICIAL USE ONLY

Security of the DFAS-Denver site is the responsibility of the site administration and contract security. The Denver Police Department provides first responder police services for this facility. During the time of this assessment, the threat level was at "ALPHA". Security is augmented by several security systems and capabilities, which have been identified as site strengths.

### Strengths:

1. The excellent condition of the overall facility.
2. The perimeter security of fencing and bollard/cable system for bomb standoff.
3. Ability to comply with DoD Forced Protection Conditions measures.
4. The contract guard service at this site.
5. Badge and vehicle decal checks at perimeter and identification checks at the building entrance.
6. Vault security through the use of CCTV and Intrusion Detection System (IDS) in place.
7. Public address communication system.
8. Building #444 has an upgraded Fire Alarm Detection and Reporting System.
9. Visitors must go through metal detectors and have carried items x-rayed.
10. Security Officer and others are attending Buckley AFB threat briefings.
11. Mailroom handling and opening process a **BEST PRACTICE**; letters and packages are x-rayed, automated letter opening is utilized and a High Efficiency Particulate Air filtration system is used. Mail handling and emergency procedures are written and trained on.

Several opportunities for improvement were identified. These were:

1. Replace the exterior lights that are burned out.
2. Conduct realistic joint fire and security exercises with first responders and Buckley Air Force Base Law Enforcement.
3. Establish a Memorandum of Understanding with Buckley AFB, which defines mutual responsibilities.
4. Perimeter security barriers – finish the bollard system on the west side of Building #444.
5. Install low lighting fixtures on existing light poles for after hour's illumination on the east parking lot.
6. Complete chain link perimeter fencing at the southeast sector along the present private wood fence and plant evergreen trees for light pollution reduction along the rear perimeter of the private homes.
7. Upgrade camera system - color enhanced digital and expand coverage to main interior corridors and east gate guard post.

**FOR OFFICIAL USE ONLY**

8. Install ballistic Mylar on south windows and maintain window coverings closed during hours of darkness and increased Alert Levels.
9. Fence both sides of east vehicle gate entrance to protect and control the movement of pedestrians on to the complex.

**F. PERSONNEL SECURITY PROGRAM:**

The Personnel Security Program was assessed by comparison of the requirements of DOD 5200.2-R, Personnel Security Program, and DFAS 3020.26R, Corporate Contingency Plan with DFAS-Denver's program implementation.

The Personnel Security Program at DFAS-DE is compliantly implemented in accordance DoD 5200.2-R and DFAS 3020.26-R. All members of the Emergency Operations Center (EOC) had current, SECRET access authorizations. 2 of 14 Emergency Management Team (EMT) personnel did not have SECRET clearances, and 4 other EMT members required Periodic Reviews. Standard Form 86s were distributed to the 4 members for completion and submission during the SPIRIT visit. Present directives do not require EMT members to have clearances. However, it is a best business practice to have the clearances due to the EMT accessing classified communications during emergencies. DFAS-DE personnel also access classified information and material due to the sites performance of accounting and finance functions for the Foreign Military Sales Program. All personnel assigned to the program had appropriate and current clearances.

The Security Briefing Program is partially implemented. The initial and terminal non-disclosure briefings were documented on the Standard Form 312 (SF 312), and new employees receive a site security orientation briefing. Additionally, Foreign Travel/Antiterrorism Level I briefing are presented to travelers. The Annual Security Refresher Briefing had not been conducted in over a year.

**G. INFORMATION SECURITY PROGRAM**

The Information Security Program was evaluated by comparison of DOD 5200.1-R, Information Security Program, requirements, with the program implementation at DFAS-DE.

The site has strongly implemented the Information Security Program requirements. All storage and protection requirements for classified and secure communications material are being met. As a best business practice, DFAS-DE has promulgated an Internal Security Standard Operating Procedure (SOP) dated January 30, 2002. The SOP specifies procedures and outlines responsibilities for the safekeeping, storage, transmission, removal, and destruction of classified material located within DFAS-Denver.

## FOR OFFICIAL USE ONLY

The current Emergency Operations Center (EOC) did not meet all requirements for a Secure Room. The EOC walls did not extend to the true ceiling, and heating/ventilation/air-conditioning (HVAC) ductwork was "man" passable. One safe needed an X.0 series lock. A new EOC is being built and was reviewed for compliance. The new EOC will be larger and better located within the DFAS-DE building for security purposes. During the SPIRIT assessment, the EOC manager located an X.08 lock for the deficient security container and submitted a work order for the replacing the lock. This deficiency is closed.

A review of the Foreign Material Sales program was also conducted. The program maintains numerous security containers and a multitude of classified documents. Similar to the EOC, all Information Security requirements were being implemented correctly.

The Information Security Assessment performed at DFAS-DE meets the DOD 5200.1R requirement for annual, Information Security assessments of subordinate units by higher authority.

### H. CONTINGENCY PLANNING /CONTINUITY OF OPERATIONS

The Contingency Planning Program was assessed utilizing the standards and requirements of DFAS 3020.26-R, Corporate Contingency Plan. Interviews were conducted with the Corporate Planner, Safety Manager, Security Officer, systems personnel, and business line personnel. Plans were extracted from the Living Disaster Recovery Planning System (LDRPS) and reviewed for currency.

The DFAS-DE contingency planning program is strongly compliant with DFAS 3020.26-R, with current plans entered into the LDRPS. Emergency, Alternate Processing, Relocation, and Continuity of Operations plans are being reviewed annually. DFAS-DE business systems are tested at the Defense Enterprise Computing Centers (DECC), which host the systems. Emergency exercises are planned, coordinated with first responders, and conducted based upon an exercise schedule. Upon completion of the exercises, after action reports with lessons learned are produced. Program deficiencies were being corrected, resulting in no opportunities for improvement observations.

### I. INFORMATION ASSURANCE (IA)

The objectives of the Information Assurance (IA) assessment were to review DFAS-Denver's implementation of DFAS Regulation 8000.1-R, DFAS Information Management Program Policy, Part G. Information Assurance Policy, requirements, evaluate compliance, and make recommendations for improvement.

## FOR OFFICIAL USE ONLY

DFAS-DE exhibits strong implementation of the DFAS Information Assurance Policies. Personnel are very security conscious. Information Systems Security Manager's (ISSM) policies and roles are implemented and IA awareness training was conducted. Password management is implemented by adherence to DoD password formulation and change requirements. Functional responsibilities are identified and implemented within the mission critical and mission essential systems. These systems have well-established security administration with strong separation of function. Functional chiefs are asked to periodically review access privileges to ensure alignment of personnel job assignments with actual system profile privileges.

Most of Denver's systems are old and have compensated for vulnerabilities through the years of service. During the operational years, vulnerabilities have been recognized and offset when necessary. Nineteen mission critical and mission essential systems were reviewed. At the time of the assessment, eleven of nineteen systems had interim or full authority to operate (ATO). As of July 31, 2003, all mission critical and mission essential systems are operating under interim or full ATO. The success of achieving DITSCAP ATO is due to a streamlining of the certification and accreditation guidelines for legacy systems, led by Lieutenant Colonel Rigotti and the Headquarters IA Team.

Several opportunities for improvement with recommendations were identified. These included:

1. Due to the extensive responsibilities and commitments of the ISSM, an assistant ISSM (AISSM) should be assigned.
2. The System Information Database (SID) role is increasing and gaining importance for scheduling and budget approval. Managers and Information Systems Security Officers (ISSO) should review and update the SID.
3. The compliance with the IA Policy for workstation lockout is poor. Workstations were continually found unlocked and with people not in attendance during facility walkthroughs. DFAS should implement default user profile with an automatic timeout to promote and encourage compliance with the DFAS workstation lockout policy.
4. During a meeting with the ISSOs, they stated little if any training was available concerning ISSO responsibilities, especially prior to assuming the ISSO. Headquarters should disseminate a training "checklist" for ISSOs, to include initial requirements for the ISSO assignment. The list should also identify recurring training requirements and professional development options.
5. The ISSOs further stated they do not receive oversight, guidance, and information from DFAS Headquarters. A forum should be devised and advertised to provide information to the ISSOs and AISSMs. An annual conference is recommended, however a website could be utilized.

## FOR OFFICIAL USE ONLY

### J. CRITICAL INFRASTRUCTURE PROTECTION (CIP)

The objectives of the CIP assessment were based upon PDD-63, Critical Infrastructure Protection and DFAS 3020.26-R, Corporate Contingency Plan. Assessment objectives were to:

1. Identify information system vulnerabilities and risks.
2. Identify a significant, single point of vulnerability.
3. Evaluate business continuity plans for contingency recovery.

CIP objectives were reviewed in conjunction with business continuity and reconstitution requirements for center site personnel using mission critical and mission essential systems. The interviewed personnel included program managers, systems managers, Technical Services Organization (TSO) personnel, and business line (functional) personnel. Reconstitution capabilities for other systems were also discussed.

Information concerning 19 mission critical and mission essential systems was collected. DFAS-DE provides system support for field sites Dayton, Limestone, Omaha, San Antonio, San Bernardino, Orlando, Japan, and Pacific. Most of the systems are old, proven, and have compensated for vulnerabilities through the years of service. The experienced support and operational staffs are valuable resources and reduce risk during a reconstitution event. As of the assessment period, seven systems were not DITSCAP accredited and certified. All systems had either full or interim authority to operate as of July 31, 2003.

Two Denver systems exhibit best business practice for continuity of operations (COOP). The Defense Joint Military Pay System (DJMS) and the Defense Integrated Financial System (DIFS) both budget and conduct COOP exercises each year. In the case of DJMS, the COOP is exercised two to three times per year.

Business reconstitution has been demonstrated by two different methods and was successful. First, business reconstitution has been replicated by scheduling vendor pay processing at various sites and eliminating the geographical restrictions. Secondly, operational events have resulted in personnel and operations being repositioned at alternate central of field sites. These events demonstrate system ability to reconstitute.

#### **Opportunities for improvement were identified:**

1. The aging systems and their experienced work force are present strengths, but become more vulnerable with age. The experience professionals are either retiring or moving to other positions, and some systems rely upon technology that is no longer supported by industry.

## FOR OFFICIAL USE ONLY

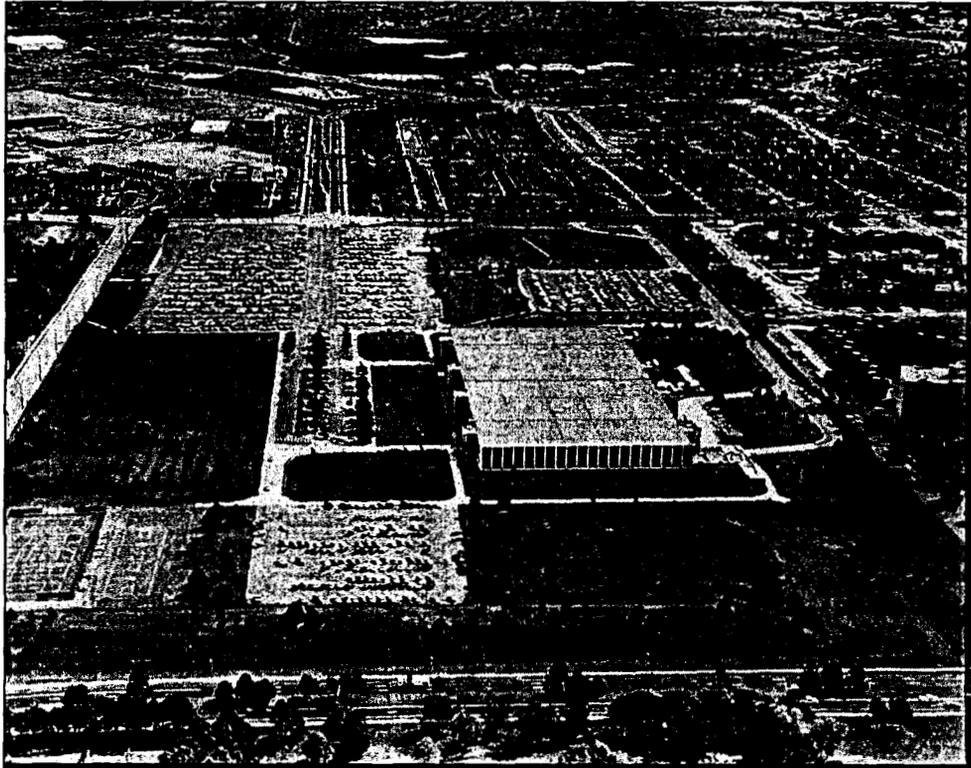
2. Some Denver systems interface directly with non-DFAS systems. For example, the Integrated Accounts Payable System (IAPS) relies upon Gunther Air Force Base for integration requirements. The service level agreement should be reviewed by systems and functional operators to ensure DFAS risks are reduced.
3. Not all systems budget for and conduct COOPs. Budgetary constraints will always exist and a more pragmatic approach should be constructed to gain COOP efficiencies.

### K. CLOSING REMARKS

DFAS-DE's program management personnel were professional, candid, and cooperative. The site was well prepared for the SPIRIT visit and had all documentation available. The SPIRIT members thank DFAS-Denver for hosting the visit, and for the hospitality extended to the Team.

Each of the report sections identifies programmatic strengths, as well as opportunities for improvement, if warranted. No grades are assigned to the programs. As stated, the SPIRIT mission objective is to benchmark the Agency wide implementation of the programs comprising SPIRIT.

Please forward all comments regarding this report to Mr. Ed Kufeldt at DFAS Headquarters, Arlington, Virginia. [ED.KUFELDT@DFAS.MIL](mailto:ED.KUFELDT@DFAS.MIL)



*Aerial View of the Building 444 Compound*



**FOR OFFICIAL USE ONLY**DFAS INDIANAPOLIS SECURITY ASSESSMENT

- DFAS Indianapolis is located in the MG Emmett J. Bean Federal Center, a General Services Administration (GSA) owned and managed facility under the jurisdiction of the Federal Protective Service (FPS), Department of Homeland Security (DHS). The facility is located in suburban northeast Indianapolis, Indiana. It consists of three stories above ground and two subterranean floors.
- As the facility is GSA owned and managed, GSA Security Alert Level measures are employed at the site as opposed to the DoD Force Protection Condition System. Contract security guards, under the management of the FPS, are the primary security force for the facility.
- Access is controlled to the interior of the facility by armed security guards utilizing metal detectors and x-ray machines.
- Delivery vehicles are screened by security personnel prior to being granted access. Incoming mail is screened in the facility's mailroom using x-ray technology.
- Closed Circuit Television (CCTV) is installed on both the interior and exterior of the facility and monitored by the on-site security force. The security force also conducts patrol activity on both the interior and exterior of the facility.
- Heating, Ventilation, and Air Conditioning (HVAC) systems are located on the roof with air intakes protected by filters. Potable water is supplied by local public utilities using an underground feed.
- DFAS last conducted an assessment (Executive Summary attached) at the DFAS Indianapolis site in August 2002. At that point in time the threat was assessed at Low to Medium dependant on the tactic assessed. A comprehensive Higher Headquarters Vulnerability Assessment utilizing the Joint Staff Integrated Vulnerability Assessment (JSIVA) methodology and benchmarks, to include standards contained in Unified Facilities Criteria (UFC) 4-010-01 (DoD Minimum Antiterrorism Standards For Buildings) is being scheduled for late FY 2005.
- Major physical security concerns identified during the August 2002 assessment included adding the Child Care Center to the Occupant Emergency Plan, and standoff. Measures taken to mitigate identified concerns include the planting of trees for barriers.

Attachment:

As stated

Prepared by: Hugh D. Wiley, (317) 510-4096

**FOR OFFICIAL USE ONLY**



---

# **Safety, Protection, Infrastructure, Recovery Integration Team (SPIRIT)**

---

## **Summary Report for Defense Finance and Accounting Service (DFAS) – Indianapolis Center**

### **FOR OFFICIAL USE ONLY**

This document contains information exempt from mandatory disclosure under the FOIA. Exemptions 2 and 5 apply.

---

***PRODUCED FOR DEFENSE FINANCE AND ACCOUNTING SERVICE BY  
TACTICAL TRAINING SPECIALISTS, LLC UNDER  
CONTRACT #MDA210-02-P-0006***

---

**FOR OFFICIAL USE ONLY****DFAS – Indianapolis Site****I. EXECUTIVE SUMMARY****A. INTRODUCTION**

In May 1998, President Clinton issued two Presidential Decision Directives, PDD-62, Combating Terrorism, and PDD-63, Critical Infrastructure Protection. The two PDDs assign responsibilities and actions associated with national level critical infrastructure protection, including physical and cyber-based systems essential to the minimum operations of the government and economy. The many terrorist attacks to the United States and its allies, culminating on September 11, 2001 at the World Trade Center Towers and the Department of Defense's Pentagon, resulted in President Bush issuing Executive Orders 13228 and 13231. The Orders require all government agencies to identify critical infrastructure elements, assess potential vulnerabilities, and implement measures to protect those critical elements.

The Defense Finance and Accounting Service (DFAS) Headquarters reviewed the collective requirements of the two PDDs and the two Executive Orders. Particular attention was addressed to Executive Order 13228's requirement for the heads of all agencies to "ensure the health and security" of their employees. DFAS responded to these requirements by identifying the key programs necessary to achieve the safety and security of its work force and infrastructure. The combination of the key programs resulted in the Safety, Protection, Infrastructure, and Recovery Integration Team (SPIRIT) concept. SPIRIT incorporates the following programs; Safety and Occupational Health, Personnel Security, Information Security, Physical Security and Anti-Terrorism / Force Protection, Contingency Planning, Information Assurance, and Critical Infrastructure Protection.

The mission objectives of SPIRIT incorporate a combined strategy. First, SPIRIT will benchmark the agency wide implementation and directive compliance for each program. During this process, SPIRIT will also identify the key infrastructure elements and the policy, procedures, and methods presently utilized to protect the key elements. Based upon this identification and benchmarking, SPIRIT will analyze the program results and offer recommendations for program improvement and vulnerability mitigation. Lastly, the SPIRIT strategy assumes the strong implementation of each of the SPIRIT programs, must be integrated, to achieve the protection of DFAS personnel, systems, and infrastructure. Program integration will be analyzed and improved by introducing training and exercises targeted to test the agency's contingency plans and readiness. The combined strategy's objective is to meet the requirements of the PDDs and Executive

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

Orders, and ensure the protection of the DFAS infrastructure and critical elements.

**B. SPIRIT VISIT DATES AND TEAM ASSIGNMENTS**

The SPIRIT Assessment was conducted August 5 – 15, 2002 at DFAS Indianapolis. The following personnel conducted the SPIRIT Assessment.

Ms. Janice Richey	Physical, Personnel, and Information Security Programs
Mr. Marvin Lewis	Physical, Personnel, and Information Security Programs
Ms. Codie Smith	Information Assurance, Critical Infrastructure Protection, and Contract Officer's Representative
Ms. Kim Ponder	Information Assurance Program
Randal Justus	Tactical Training Specialists LLC (TTS) Team Lead, Personnel Security, Information Security, and Contingency Planning Programs
Eva Jean Bryson	Safety and Occupational Health Programs
John Devico	Physical Security, Anti-Terrorism / Force Protection
Bret Aduddell	Physical Security, Anti-Terrorism / Force Protection
Charles Butler, Ph.D.	Information Assurance and Critical Infrastructure Protection

**C. DFAS INDIANAPOLIS SITE DESCRIPTION AND BACKGROUND**

DFAS Indianapolis is located in the northeast quadrant of Indianapolis, Indiana on the former Fort Benjamin Harrison site. The primary building occupied by DFAS Indianapolis is the Major General Emmett J. Bean Federal Center at 8899 East 56<sup>th</sup> Street. The Bean Federal Center is a General Services Administration (GSA) owned and managed facility, of approximately 1,600,000 square feet. DFAS Indianapolis shares the Bean Federal Center with other government tenants.

The GSA maintains and protects the Bean Federal Center. Performing those tasks has been a major challenge the past four years during the major renovation of the facility, especially considering the estimated building occupancy of 3,700 personnel during the renovation. Tenant missions have been sustained during the renovation, by either shuffling personnel and activities around the Bean Center or leasing temporary space for the personnel and activities. At present, DFAS Site Management and other functions involving about 300 DFAS personnel are located at the Theodore Roosevelt Building (a GSA leased facility). The renovation activities and resulting turmoil have been a significant and constant challenge to the security and safety programs.

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY****Major General Emmett J. Bean Federal Center**

DFAS Indianapolis facilities also include a warehouse. Both Safety and Security walkthrough assessments were accomplished in the warehouse. The Safety concerns will be addressed, but the security threats to the warehouse were considered to be only standard industrial security issues. Given the pending move of DFAS Indianapolis personnel from the Theodore Roosevelt Building, and the minimum, security threat to the warehouse, neither facility will receive significant assessment consideration from the security program reviews.

**D. SAFETY AND OCCUPATIONAL HEALTH PROGRAM**

Managing the Safety and Occupational Health Programs during the major renovation of the Bean Federal Center has been a monumental challenge to both the GSA and DFAS Indianapolis Safety and Occupational Health professionals. Given the many challenges, the overall programs are satisfactorily implemented.

The most significant DFAS Indianapolis'- Safety and Occupational Health program issues and requirements are to:

- Formalize the Safety and Occupational Health programs by issuance of a written policy. Currently the policy is in draft, and earlier revisions were not available. The written policy must include Hazard Communication, Personal Protective Equipment, Safety Inspection, and Ergonomics Programs as a minimum.
- Update the master list of Material Safety Data Sheets (MSDS) and obtain/retain the MSDS on site for all chemicals present in the Bean Federal Center and the warehouse facility.

**FOR OFFICIAL USE ONLY**

### **FOR OFFICIAL USE ONLY**

- Conduct and document Employee Safety Training.
- Establish, formalize and implement a facility Safety Committee Program comprised of all tenants within the Bean Federal Center.
- Post the annual accident/injury summary and Workplace Poster (OSHA Publication 3165).
- Formalize the Personal Protective Equipment (PPE) program, to include performing job hazards analysis to determine necessary PPE, and post requirements in the work area.
- Establish an Ergonomic Evaluation Program to evaluate workstations.

#### **E. PHYSICAL SECURITY, ANTI-TERRORISM / FORCE PROTECTION PROGRAMS**

Security of the Bean Federal Center is the responsibility of the General Services Administration (GSA) and the Federal Protective Service (FPS). The FPS provides around the clock, armed guards. The guard service is augmented by several security systems and security capabilities such as:

- Badge and access control system
- Perimeter and internal camera system with recording capabilities
- Standoff from parking areas and access routes
- Delivery vehicle checks by guards
- Strong structure with newly installed security features
- Limited access portals with state-of-the-art magnetometers and x-ray equipment for personnel and package scanning
- Ability to fully implement 37 of 39 GSA Security Alert Level requirements, and partially implement the remaining 2
- Excellent cooperation and security awareness from building occupants
- Excellent emergency planning

Three opportunities for improvement were identified. These were:

1. The Childcare Center, located within 150 feet of the Bean Federal Center (BFC) is GSA owned, contractor operated, and open to the general public. Currently, the Childcare Center is not included in the BFC Occupant Emergency Plan (OEP), even though the Childcare Center's primary emergency response, per GSA, is to evacuate to the BFC. Given the potential for hostage situations at the Childcare Center, (though rated as Moderate) and other emergency scenarios involving the Childcare Center, the BFC OEP should be expanded to include contingency plans for those scenarios.

### **FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

2. The Roosevelt Building is a significant security problem and susceptible to numerous Terrorist Threat Scenarios. Moving DFAS Indianapolis personnel from the Roosevelt Building to the BFC as soon as possible will mitigate the potential scenarios and focus resources on the BFC.
3. Perimeter vehicle barriers are incomplete and could allow high speed vehicle access for Terrorist's scenarios. Completing the perimeter barriers will provide the desired security standoff and mitigate vehicle bomb threats. The use of trees, planters, ditches, and other types of landscaping barriers is recommended.

**F. PERSONEL SECURITY PROGRAM**

The Personnel Security Program at DFAS Indianapolis was evaluated by comparison with the requirements of DOD 5200.2-R, Personnel Security Program and determine local program compliance with the regulation. The following opportunities for improvement were identified:

- Not all personnel assigned to the Emergency Management Team had SECRET access authorizations as required by DFAS 3020.26R.
- Personnel in positions meeting the DOD 5200.2-R criteria for Critical/Sensitive and Non-Critical Sensitive positions do not have the required background investigations, or have not been processed for the required Periodic Reviews.
- Managers, Human Resource Specialists, and Security Specialists should be trained to evaluate position sensitivity utilizing the criteria of DOD 5200.2-R.
- DFAS Personnel Security Program Manager (Headquarters) should revise the DFAS Form 113 to capture all the sensitive position criteria required by DOD 5200.2-R.
- Personnel entering data and utilizing the Personnel Security Database (PSD) should be aware of the potential to incorrectly enter or interpret the position sensitive classifications, as the classifications are reversed as compared to the ratings of the Automated Data Position ratings in DOD 5200.2-R. As an example, the PSD classification identifier for a Critical/Sensitive position is a "3" while the regulation classification for Critical/Sensitive Automated Data Processing position is "ADP 1". Either incorrectly entering or misinterpreting the rating could lead to unauthorized access by non-cleared personnel.

**G. INFORMATION SECURITY PROGRAM**

The Information Security Program at DFAS Indianapolis was evaluated by comparison with the requirements of DOD 5200.1-R, Information Security Program. The following program issues were identified:

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

- Classified automated information system material (Personal Computers used to process classified information, removable hard drives, and diskettes) was not labeled with the highest security classification of the information contained in the media.
- End-of-the-day security checks were not being performed and documented as required by regulation. This deficiency was corrected during the assessment period.

The DFAS Indianapolis Security Education Program was well implemented, covered all Security programs, and met regulatory requirements. The Security webpage is excellent!

### H. CONTINGENCY PLANNING /CONTINUITY OF OPERATIONS

The Contingency Planning Program was assessed utilizing DFAS 3020.26-R, Corporate Contingency Plan. The DFAS Indianapolis Contingency Planning Program is the strongest program reviewed to date. The Planning Team has developed standardized plans to be utilized DFAS wide, and the plans only require site specific information be added to be fully functional. The standardization of plans enhances the Agency's ability to train and exercise contingency teams and individuals.

Observations of the Contingency Planning Program included the following:

- The Occupant Emergency Plan was well documented and exercised. A need was identified to include the Child Care Center (even though it is a GSA owned and contractor operated facility) in the plan.
- Exercise plans are developed and utilized to conduct exercises. The exercise results were documented in After Action Reports.
- Business Process Recovery Plans were developed and entered in the Living Disaster Recovery Planning System (LDRPS) as required by the DFAS Contingency Planning Regulation.
- Automated Information System (AIS) contingency plans were developed prior to January 2002 (Y2K), and are due for updating.
- The DFAS 3020.26-R required testing program (consisting of Paper, Table-top, and Live Tests) is not fully implemented. This is a common observation from all sites assessed to date. DFAS management should focus on ensuring the testing program is fully implemented throughout the Agency. Developing a three-year schedule to include all test requirements and including the testing implementation on the Balanced Score Card may be a mechanism to ensure the testing program is fully implemented.
- The Emergency Operations Center was fully operational in all respects.
- An Emergency Action Plan (EAP), to protect classified material (to include classified communications keying material) had not been developed. To the credit of the Planning Team, a DFAS standardized

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

EAP was developed and sent out to all DFAS sites. The Team deserves kudos for their initiative.

### I. INFORMATION ASSURANCE (IA)

The assessment objectives of the Information Assurance (IA) were to determine:

- The training and awareness levels of DFAS employees and personnel assigned key system administration and security functions according to the DFAS Corporate IA Program (DFAS Regulation 8000.1-R, Part G.).
- The vulnerabilities of the DFAS automated information systems (AIS) through the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) and promote completion of the process for each DFAS system identified as mission critical or essential.

The assessment was conducted by interviewing the DFAS-Indianapolis Information System Security Manager (ISSM), Information System Security Officers (ISSO), and key personnel managing and using 19 Information Systems identified as mission critical or essential. Meetings were conducted with the key personnel, where the SPIRIT IA team reviewed password management within the Center Site and between Indianapolis and the field sites using the systems. The 19 mission critical/essential systems were reviewed for System Security Authorization Agreement (SSAA) certification status.

The following IA Policy compliance observations were made:

- The key systems personnel exhibited awareness of IA roles and policies for password formulation, password management, workstation lockout, and ISSM and ISSO responsibilities.
- ISSM's and ISSO's were assigned with letters on file for formal authorization.
- Password policies and procedures were implemented for the 19 systems. When standard password formulation was not achieved, it was based upon technical restrictions and noted in the risk assessments. When password formulation policy was violated, the exception was identified and documented within the system risks documentation.
- As observed by walking around the DFAS Indianapolis work areas, when personnel were absent from their work place, workstation lockout was implemented and policy adherence was observed. Employees appeared to have a good understanding of the IA password and lockout policy

The following observations were made concerning System Security Authorization Agreement (SSAA) status for the 19 mission critical and essential systems.

- No mission critical or essential systems have full accreditation. Below is a summary of the accreditation status for 19 mission critical or essential Indianapolis systems:

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

No progress in obtaining accreditation	8
Developing the accreditation package	5
Accreditation package is being staffed for approval	2
Interim accreditation has expired	2
Currently are interim accredited	2
Full accreditation	0

- Knowledge regarding the status of individual system accreditation was mixed. Selected personnel were aware of a lack of accreditation and cited budget constraints. Other personnel were not aware of the accreditation goals.
- The DITSCAP process for accreditation was cited as a low priority and budget funding restrictions contributed to low SSAA accreditation.
- A growing inventory of site-developed applications was found. These applications augment functional operation of mission critical or essential systems. The development and maintenance of this inventory is not formally included in IA policies.
- The system inventory is expanding with mid-tier systems. Some of these systems reside operationally in the Infrastructure Services Organization (ISO), not the Defense Enterprise Computer Centers (DECC). IA policies for mid tier systems, especially those not residing at a DECC, should be reviewed for currency and new operational environments to ensure backup and recovery and business continuity

**J. CRITICAL INFRASTRUCTURE PROTECTION**

The Critical Infrastructure Protection assessment objectives were based upon PDD-63, Critical Infrastructure Protection and DFAS 3020.26-R, Corporate Contingency Plan. Assessment objectives were:

- Identify information system vulnerabilities and risks
- Identify a significant, single point of vulnerability
- Evaluating business continuity for contingency recovery

The following observations were made affirming CIP preparedness for the central site and its 19 mission critical and essential systems:

- DECC and central site working partnership is strong including backup and recovery, and data replication.

**FOR OFFICIAL USE ONLY**

## FOR OFFICIAL USE ONLY

- Living Disaster Recovery Planning System (LDRPS) is populated with contingency plans. Most of the content is Y2K derived and might not be applicable today
- Continuity of Operations Plans (COOP) are executed and selected post evaluations are conducted.
- Contingency planning is conducted including business function links.
- ISO architecture is partially duplicated in Columbus.
- Selected systems are Software Engineering Institute (SEI) Capability Maturity Model (CMM) certified.

The following observations were made concerning CIP preparedness for the central site:

- Deployment of systems on the Infrastructure Services Organization (ISO) architecture and replication of service level agreements (SLA) for business continuity. Selected DFAS systems are deployed on ISO infrastructure rather than DECC architecture. Internal service level agreements with DFAS ISO should contain corresponding or higher security and contingency recovery requirements as implemented in DECC service level agreements.
- Inventory of home grown or site specific applications that serve as workarounds or augment systems. With budget and other operating constraints, DFAS personnel have written software that augments existing systems. This software is now a part of the "operational procedures" without formal identification or management and should be inventoried.
- Volume of DFAS "corporate" documents (critical asset) that support DFAS processes and operation. DFAS assets, other than systems, are growing, particularly in the area of internal documents and knowledge. The management of these documents should be formalized and adequate backup and recovery should be implemented.
- Participation of existing functional and technical personnel with development personnel responsible for new systems replacing legacy. In the case where systems are categorized as legacy for planned decommissioning, current functional and technical personnel are not active participants in the development of new systems. The knowledge of the personnel should be transferred to the new systems to insure business continuity with deployment.
- Service levels with Defense Enterprise Computer Centers (DECC) to comply with DFAS 3020.26-R Corporate Contingency Plan. The DFAS 3020.26-R required testing program (consisting of Paper, Table-top, and Live Tests) does not parallel the service levels prescribed with DECC. This inconsistency should be reviewed to identify and implement efficiencies for Continuity of Operation Plans (COOP).
- Staffing dependency upon long term employees who are eligible or will be eligible soon for retirement. As with previously visited central and field

## FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**

sites, key personnel are entering or approaching a retirement window. Critical system support and operations should be revisited and gauged against the personnel retirement opportunities to ensure that knowledge and expertise is transferred in planned progress.

**K. CLOSING REMARKS**

DFAS Indianapolis program management personnel were professional, candid, and cooperative. The SPIRIT team members thank DFAS Indianapolis for hosting the visit, and for the hospitality extended to the Team.

Each of the report sections identifies opportunities for improvement, if warranted. No grades are assigned to the programs. As stated, the SPIRIT mission objective is to benchmark the Agency wide implementation of the programs comprising SPIRIT.

Please forward all comments regarding this report to Mr. Ed Kufeldt at DFAS Headquarters, Arlington, Virginia. ED.KUFELDT@DFAS.MIL

**FOR OFFICIAL USE ONLY**