AIR WAR COLLEGE

AIR UNIVERSITY

ARGUMENT FOR A JOINT SAFETY REPORTING SYSTEM

by

Mark Nunn, GS-14, DAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Roy F. Houchin II

13 February 2015

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
13 FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Argument For A Joint Safety Reporting System	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College,,Air University,,Maxwell AFB,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On-duty operations and off-duty activities of service members, account for the majority of mishaps experienced by the Department of Defense (DOD). Due to the importance of mishap prevention, the services developed separate safety data collection and reporting systems (referred to as safety data system(s) from this point forward) to support this effort. Current systems are stovepiped with little to no linkage or standardized architecture. This paper uses a qualitative approach to illustrate the benefits of selecting the AF Safety Automated System (AFSAS) as the joint-service safety data system for the services and DOD.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT	b ABSTRACT	c THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**29**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

GS-14, Mark Nunn is assigned to the Air War College, Air University, Maxwell AFB, Alabama. Mr. Nunn was previously assigned as the Chief of the AF (AF) Automated System (AFSAS) Requirements Group, and as the AF Risk Management (RM) Process Manager for the HQ AF Safety Center (AFSEC) at Kirtland AFB, New Mexico. His primary duties included leadership and oversight of the day-to-day sustainment and future requirements development of the AFSAS program, as well as overall Program Management responsibilities for the AF RM Program serving 690,000 active-duty, Guard, Reserve and civilian forces worldwide.

Mr. Nunn entered the AF in 1986 following graduation from California Polytechnic University, Pomona California via his commission through the AF ROTC program at the University of Southern California. During his 22 years of active duty, he served as a C-141B Aircraft Commander and Schoolhouse Instructor Pilot, a Chief of Wing Current Operations, a C-20B/C and C-37A Special Missions Aircraft Commander. He also held key staff positions at Headquarters Air Mobility Command - Operations Training Division, and Headquarters AF Safety – Flight Safety Division, and Analysis and Integration Division. As a former Command Pilot with over 4,000 flying hours, he led numerous missions supporting Operations JUST CAUSE, DESERT SHIELD/STORM, NOBLE EAGLE, IRAQI FREEDOM and ENDURING FREEDOM.

Mr. Nunn retired from active duty in March 2009 and immediately returned to Government Civilian Service with AF Safety in April 2009 where he served until his assignment to Air War College in July 2014.

Abstract

On-duty operations and off-duty activities of service members, account for the majority of mishaps experienced by the Department of Defense (DOD). Due to the importance of mishap prevention, the services developed separate safety data collection and reporting systems (referred to as safety data system(s) from this point forward) to support this effort. Current systems are stovepiped with little to no linkage or standardized architecture. This paper uses a qualitative approach to illustrate the benefits of selecting the AF Safety Automated System (AFSAS) as the joint-service safety data system for the services and DOD. It presents an overview of the mishap data-collection process and the similarities and differences in "why, what and how" data is collected. It also conducts a macro-comparison of the specific capabilities and limitations of each system. Discussion of the Goldwater-Nichols Act of 1986, the Federal Data Center Consolidation Initiative (FDDCI), the DOD Information Technology (IT) Enterprise Strategy Roadmap, and the "Cloud First" policy highlight challenges of future development strategies. Finally, a future vision comparison of the AF and U.S. Navy (USN) systems clearly illustrate the AF Safety Automated System (AFSAS) is the system of choice for the joint-service safety data system. Four primary recommendations support this choice: 1) Create a joint program office to oversee the joint-service safety data-collection system and leverage joint-service personnel and funding to support development and quality control requirements for migration of required data from these agencies into the joint system; 2) Build comprehensive requirements and functionality into the joint-system to accommodate the data sets and unique differences of the included DOD components and agencies; 3) Develop service team leads to train appropriate personnel with the system prior to use; 4) Continue to develop capabilities, and streamline functionality as necessary to meet future DOD component and agency needs.

"The Goal is to turn data into information, and information into insight."
Carly Fiorina, Former CEO of HP

Introduction

Two AF F-15s above the East China Sea, conducting Basic Fighter Maneuver and air refueling training, are awaiting a rejoin with the remaining flight members when distraction leads to a mid-air collision; both pilots safely eject but the jets crash into the sea. An Army M1240 M-ATV, with an inexperienced operator and three passengers, approaches an unfamiliar river crossing. During the crossing the vehicle is overcome by the river forces and overturns; all personnel are lost and the vehicle is heavily damaged. An off-duty Marine, while riding his motorcycle on a winding road loses control, crashes, destroys the bike, and incurs major injuries. What is the commonality among each of these unrelated events? They are all examples of DOD and U.S. military service reportable "on/off-duty" mishaps.[1] Due to the importance of mishap prevention, the services maintain professional safety staffs to identify hazards, address root causes of mishaps, and provide strategies to mitigate or eliminate mishaps. Evolution of investigative procedures, coupled with the need to compile and collate data for analysis, led to the development of separate mishap data collection and reporting systems (referred to as safety data system(s) from this point forward) within the services. The problem is these systems are stovepiped, service-specific, and have little to no linkage or standardization among them. This lack of interoperability makes it difficult to efficiently collect, collate, or compare comprehensive hazard and mishap data within and across the services. System differences, coupled with non-standardized data fields, create delays in cross-service data analysis, trending, and implementation of mishap mitigation strategies. In addition, current fiscal realities, coupled with federal policies focused on streamlining government operations, as well as reducing

duplicative IT systems, are driving the DOD and military services to improve processes to save time, resources and manpower. A background review of why, what and how mishap data is collected, coupled with a macro view of current safety data systems, a discussion of the challenges of future development strategies, and the future vision of capabilities and cost effectiveness of a single joint safety data system will clearly illustrate the AF Safety Automated System (AFSAS) is the system of choice for the joint-service safety data system.

BACKGROUND

Why mishap data is collected

Over the past 50 years, technological advances, improved systems, and better reliability in hardware have contributed to significant reductions in overall mishaps and mishap rates.[2] However, despite these improvements, we have not found a way to effectively engineer human factors out of the equation when it comes to mishaps. As an example, it is estimated 67% of AF aviation related mishaps as well as 85% of ground related mishaps are directly related to human factor failures; not mechanical anomalies.[3] In an effort to identify the hazards and the root causes for these mishaps, the military services take great efforts to investigate these accidents, gather data, and analyze the findings to mitigate or eliminate causes where possible. Department of Defense Instruction (DODI) 6055.07, *Mishap Notification, Investigation, Reporting, and Record Keeping,* 6 June 2011, establishes the requirements for safety and occupational health data collection and reporting.[4] The instruction applies across all DOD components, and its purpose is to "Protect DOD property from damage and DOD personnel from accidental death, injury, or occupational illness" as well as "Protect the public from the risk of death, injury, illness, or property damage because of DOD activities."[5] Beyond the guidance, commanders and leaders

clearly understand the importance of a strong, effective, safety program for saving lives and preserving combat resources.

What mishap data is collected?

Mishap data associated with Class A-D mishaps, Class E & F events (service dependent), and other related events, constitute the majority of the information collected by the services for hazard identification as well as mishap prevention and analysis. DODI 6055.7 defines Class A-D mishaps as follows:

1. **Class A:**
    a. Direct mishap cost totaling $2,000,000 or more.
    b. A fatality or permanent total disability.
    c. Destruction of a DOD aircraft (Excluding RPA groups 1, 2, or 3)
2. **Class B:**
    a. Direct mishap cost totaling $500,000 or more but less than $2,000,000.
    b. A permanent partial disability.
    c. Inpatient hospitalization of three or more personnel. Do not count or include individuals hospitalized for observation, diagnostic, or administrative purposes that were treated and released.
3. **Class C:**
    a. Direct mishap cost totaling $50,000 or more but less than $500,000.
    b. Any injury or occupational illness causing loss of one or more days away from work not including the day or shift it occurred.
4. **Class D:**
    a. Direct mishap cost totaling $20,000 or more but less than $50,000.
    b. Any mishap resulting in a recordable injury or illness not otherwise classified as a Class A, B, or C mishap.[6]

Air Force Instruction (AFI) 91-204, *Safety Investigations and Reports*, Army Regulation (AR) 385-10, *The Army Safety Program*, and Coast Guard Commandant Instruction (COMDTINST) M5100.47A, *Safety & Environmental Health Manual*, also discuss Class E & F events as:

5. **Class E & F Events:**
    a. Certain occurrences do not meet reportable mishap classification criteria, but are deemed important to investigate and report for hazard identification and mishap prevention.[7]

DODI 6055.07 also establishes the minimum standard data elements all DOD Components are required to collect in relation to these mishaps. The collection of these standard elements

ensures, "…accurate mishap trending, efficient hazards analysis and more efficient sharing of lessons learned."[8] Accordingly, there are six major mishap categories (Afloat, Aviation, Ground [Ashore], Motor Vehicle, Space, and Weapons) and 23 associated sub-categories outlined in the DODI forming the basis of all safety and occupational health datasets.[9] In addition, the data is mandated to include human error data using a, "common human error categorization system that involves a human factors taxonomy accepted among the DOD Components."[10] This current taxonomy is captured in the DOD Human Factors Analysis and Classification System (HFACS) Guide implemented in January 2005 via an associated Memorandum of Agreement between the services on the use of the HFACS taxonomy.[11]

Moreover, the minimum data elements are constantly evaluated and refined by the DOD Safety Information Management Working Group (SIMWG). This group ensures commonly collected data fields are relevant and meet the requirements of DODI 6055.07, other mandated reporting requirements across DOD (i.e., the DOD Explosive Safety Board [DDESB]), as well as specific Occupational Safety and Health Administration (OSHA) requirements for the OSHA 300 and 300A, *Log and Summary of Work-Related Injuries and Illnesses reports*.[12] In 2008, the SIMWG increased the number of common data elements to 118, to meet the safety needs across DOD and OSHA.[13] The SIMWG is currently reviewing this list and expects the number of fields to reduce once the services come to a consensus on the final list; however, there is currently no projected timeline for this change. Beyond strict mishap related and human factors data collection, the services also track hazard data not directly associated with mishaps or injury. This precursor data is important for effective risk management in conjunction with proactive mishap prevention.

Each military service also manages formal risk management (RM), risk assessment programs, safety inspection programs, and hazard abatement programs contributing to the safety awareness and well-being of their personnel.[14] Although these programs provide effective processes for RM and safety awareness, they are not integrated with the safety data collection systems of their respective service.

How mishap data is collected

Collection of mishap data is accomplished in multiple ways across the services, but always originates from the initial report of a mishap. Formal mishap reporting is accomplished through specific processes and procedures outlined in DODI 6055.07, as well as service-specific guidance: (Air Force) AFI 91-204, *Safety Investigations and Reports*; (Army) AR 385-10, *Army Accident Investigations Reporting*; (Navy/Marines) Chief of Naval Operations Instruction (OPNAVINST) 5102.1D, *Navy & Marine Corps Mishap and Safety Investigation, Reporting and Record Keeping Manual*; OPNAVINST 3750.6S, *Naval Aviation Safety Management* System; (Coast Guard) Commandant Instruction (COMDTINST) M5100.47A, *Safety and Environmental Health Manual*.[15] Additionally, the services breakdown reporting and investigation procedures into the respective functional areas: Afloat, Aviation, Ground, Weapons, etc. Service-specific publications provide guidance and procedures associated with mishaps in each area.

Despite specific differences in investigative process, there are essentially three primary ways mishap reporting is accomplished across all of the services: direct reporting of mishaps to safety personnel via phone calls, authorized forms or hand written reports turned in to safety offices for action, or through direct entry of mishap data into the safety data system. Regardless of how it is reported, once a mishap report is received and validated, all required information is entered into the service's safety data system for future review, analysis, and trending.

Unfortunately, there is little standardization amongst the services on the collection processes for mishap data, and in many cases functional areas and/or specific hazard data bases are stovepiped making collation and comparison difficult.

MACRO VIEW: CURRENT SAFETY DATA SYSTEMS

> **Note:** The following overview of current safety data systems assumes all are compliant with federal and DOD security requirements.[16]

Army

The U.S. Army (USA) currently utilizes the Army Safety Management Information System (ASMIS) as its primary repository for all USA reportable accidents and associated data. ASMIS is locally hosted at the Army Combat Readiness/Safety Center (USACR/SC) on centralized servers. It is a Common Access Card (CAC) accessible system closed to the general public. Access by other service users and safety professionals is approved on a case-by-case basis via ASMIS gatekeepers only. All primary data entry to this system is made by assigned personnel at the USACR/SC as transcribed from formal reports and forms available at their website.[17] In all cases, Army safety investigators utilize these forms to report and document mishap information. Once complete, they forward the forms to the USACR/SC for processing and entry into ASMIS; currently, there is no direct field entry of investigative data into ASMIS. This inefficient practice leads to delays in the timely update of mishap data into the ASMIS database.

Also linked to ASMIS, and hosted on the USACR/SC homepage, is the Army's web-based Risk Management Information System (RMIS). RMIS allows approved users to conduct searches on reported mishaps (Class A-D, ground on/off-duty Class A-E, aviation) to obtain risk and hazard reports broken down by "age, grade, equipment, and additional fields.[18] The RMIS

provides “Excel” type data retrieval only with no ability to conduct advanced mishap data analysis reporting, graphing or comparisons.

In addition, there is a third opportunity, the web-based Army accident reporting system, called “ReportIt,” hosted on the USACR/SC. Mandated for use in FY12, ReporIt, “was created to assist the Army in meeting its requirements in AR 385-10, to capture all military, civilian, and contractor incidents and report/record those incidents within a centralized repository.”[19] Per the site, ReporIt was implemented to address problems of under-reporting of mishaps and events. The application requires CAC approval to access and utilizes a “Turbo-Tax” type interface to guide users through the report submission process only. The interface is strictly for reporting and does not provide any data query, retrieval, or analysis capability.

Air Force

The AF utilizes the web-based AF Safety Automated System (AFSAS) as its primary repository for all AF reportable accidents and associated data. On 28 March 2014, AFSAS migrated from centralized servers hosted at AFSEC to a commercial cloud, Virtual Private Cloud (VPC) environment. It is a CAC accessible system closed to the general public. Access by other service safety professionals is approved on a case-by-case basis via AFSAS approved gatekeepers. Data entry into this system is made directly by authorized safety professionals, mishap investigators, and occupational health & safety professionals through online entry only; no third party transcription is conducted at AFSEC for the field users. Although AF mishap reporting forms are available as required on the AFSEC webpage or the AF electronic publications site, all AF mishaps and reportable personal injuries are documented directly on-line via AFSAS whenever possible.[20]

AFSAS is a one-stop application for Class A-E mishap reporting across all disciplines, with "Turbo-Tax" type entry. The system provides the means to document all required Safety Investigation Board (SIB) Tabs and information within the system for Quality Control, review, approval, and final release by appropriate convening authority personnel. The system also provides authorized users the ability to search documented mishaps, create individual ad-hoc queries, conduct detailed comparative analysis, as well as produce graphs and charts via data extraction and business intelligence tools imbedded within the AFSAS application. In addition, occupational health specialists have separate and distinct AFSAS account access to query occupational illness investigations, produce occupational illness reports, and/or automated OSHA 300 and 300A reports within the AFSAS report tab as required.

Navy & Marines

The U.S. Navy (USN) and U.S. Marine Corp (USMC) utilize the Web Enabled Safety System (WESS) as their primary repository for all USN and USMC reportable accidents and associated data. WESS is locally hosted at the Naval Safety Center (NAVCEN) via centralized servers. WESS is a CAC accessible system closed to the general public. Access by other service safety professionals is approved on a case-by-case basis via WESS gatekeepers only. Primary data entry to the system is via a "Turbo-Tax" style interface by authorized field personnel when accessible; however, due to connectivity issues related to "Afloat" or disconnected contingency operations, electronic entry is not always possible. In these cases, investigative personnel are directed to utilize Naval Operations (OPNAV) forms 3750/59 *through* 69, to document mishap information for aviation related mishaps. Subsequently, these forms are forwarded via email to the designated authority directed in OPNAVINST 3750.6S, for input into the WESS Aviation Mishap and Hazard Reporting System (WAMHRS).[21] For non-aviation related mishaps, users

have the option to use the off-line WESS disconnected system (WESS-DS) via email or to submit a report using the naval message format directed in OPNAVINST 5102.1D.[22] In these cases, NAVCEN personnel enter the data into WESS for action, future reference, and analysis.

The Navy's Enterprise Safety Applications Management System (ESAMS) is a separate web-based, CAC enabled system for reporting minor occupational safety and health (OSH) related events. ESAMS reports are forwarded to the NAVCEN for review and, if determined to be anything other than minor OSH events, get kicked back to the submitter for entry into WESS. ESAMS allows the Navy to comply with OSHA and OSH reporting requirements.

Coast Guard

The U.S. Coast Guard (USCG) utilizes "e-MISHAPS" for all reportable non-aviation (Afloat & Ashore) mishaps and "e-AVIATRS" for reportable aviation mishaps. These two applications provide the primary repository for all USCG reportable accidents and associated data. These applications are locally hosted by the USCG via centralized servers. The systems are web-based, password protected but non-CAC enabled for access. Access is controlled by USCG gatekeepers; but, the site is accessible to the general public. Although the USCG has a mishap report form (CG-5584, *U.S. Coast Guard Mishap Report*), there is no guidance in COMDTINST M5100.47A for its use in the event the web-based systems are unavailable.

DOD

The DOD has a single system acting as a gathering point for the services common data elements for mishap information. This system, referred to as the Force Risk Reduction (FR2) database, is maintained by the DOD SIMWG. According to Mr. Donald "Deke" Forbes, Senior System Analyst and Military Mishaps Functional Lead and Navy-Marine Corps Subject Matter Expert (SME) for the SIMWG, the DOD Force Risk Reduction system rolls up the service safety

data into standard or common (or what should be standard, based on the policy provided in 2008) data elements for ease of comparison. According to Mr. Forbes, FR2 is a safety collection system only; it simply receives mishap data from the other services.[23] The limited system does not provide users with the ability to search full mishaps reports, create individual ad-hoc queries, conduct detailed comparative analysis, or produce graphs and charts.

THE CHALLENGES OF FUTURE DEVELOPMENT STRATEGIES

Although the services have similar safety data systems, there is no established crosstalk or data sharing among the service systems other than the minimal push of common mishap data elements to the FR2 system. This data is only a small fraction of the total mishap collected by each service; FR2 does not have the functionality or scope to assist in detailed safety analysis necessary for effective mishap prevention and hazard abatement. The challenge for developing a single, joint-service safety data system is tied to decades of interservice rivalry, parochial thinking, and historically stovepiped development efforts by the services. However, recent policies focused on eliminating redundancy, streamlining IT systems, and leveraging technology to make systems more economical and efficient highlight the way for a joint-service safety data system.

The Goldwater-Nichols Act of 1986 was the first formal effort to improve relations between the services and to direct the Chairman of the Joint Chiefs to consider achievement of "maximum effectiveness of the armed forces" in part by considering "unnecessary duplication of effort among the armed forces" as an avenue to direct change when such duplication exists.[24] Although primarily focused on changing how the services organize, train, and equip their forces, this same guidance is applicable to the duplicative IT systems across the federal government and DOD; and, specifically, to the safety data systems discussed here.

On 26 February 2010, Vivek Kundara, Federal Chief Information Officer (CIO), released a memorandum to all federal and DOD-level CIOs introducing the Federal Data Center Consolidation Initiative (FDDCI).[25] This initiative focused on four primary issues: 1) the use of Green IT and reduction of energy and physical footprint of data centers; 2) cost reductions of data center hardware, software, and operations; 3) increased IT security of the government; 4) to shift investments to more efficient computing platforms and technologies.[26] The majority of the safety data systems continue to operate on legacy platforms and technology and need to embrace modernization and efficiency to meet the intent of the FDDCI.

On 6 September 2011, the DOD released the DOD IT Enterprise Strategy Roadmap to address DOD network and infrastructure issues. Teri M. Takai, the DOD CIO stated, "… the incremental and evolutionary manner in which DOD develops information technology (IT) has resulted in layers of stove-piped systems that are difficult to integrate and not as effective as needed."[27] As well as, "Aggressively consolidating now will better position us to embrace emerging technology and provide cutting-edge service to our warfighters. This aggressive consolidation cannot, however, come at the price of degraded capabilities for the warfighter or inflexible commitment to a specific technological solution."[28] The consolidation of the service safety data systems fits nicely into the DOD strategy as these systems provide similar functionality to their users and consolidation would eliminate redundant systems and increase overall data access as well as reporting capabilities for all services.

Additionally, on 8 February 2011, the U.S. CIO released the Federal Cloud Computing Strategy, instituting the "Cloud First" policy: "Following the publication of this strategy, each agency will re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process. Consistent with the Cloud First

policy, agencies will modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost."[29] The elimination of host server farms and associated maintenance requirements for the service safety data systems by migration of these systems to a cloud-based application will save the services and DOD hundreds, if not thousands, of dollars in annual maintenance, hardware refreshment, and manpower costs; consolidation to a single-system would further increase these cost savings.

Coupled with the current fiscal environments of budget and manpower reductions, the DOD and service safety data systems fit neatly into consideration for streamlining and consolidation due to their similar functionality and overall purpose for mishap data collection, trending, and analysis. Although services contend they are unique in their data collection requirements based upon their specific operating environments as well as mission sets, the reality is regardless of how or where a mishap occurs, or a hazard is identified, the functionality of collecting, inputting, trending, and analyzing the data is virtually identical regardless of service.

FUTURE VISION OF CAPABILITIES AND COST EFFECTIVENESS

Baseline comparisons of the services reveals only the AF and Navy are seriously seeking evolutionary improvements in their current safety data systems to meet future needs; but, there are differences. While the AF modifies and updates the AFSAS program to meet current requirements, and to comply with the FDDCI, the Enterprise Strategy Roadmap and the Cloud First policy, the Navy is initiating a full-scale program change via the development of a new Risk Management Information (RMI) system to replace WESS.[30]

According to the Navy's "As-Is" analysis to support the RMI development: "Current SOH and risk management systems and processes have not been sufficient in providing the tools

required to implement process improvement, reduce mishaps, or lower the cost associated with risk management and mishap loss. As such, the goals and objectives directed by the Office of Secretary of Defense (OSD), DASN (Safety), COMNAVSAFECEN, and CMC SD, will not be achieved without changes to current processes supported by technology."[31] They define root causes for these problems as:

1) Stove-piped capabilities, processes, and data, hinder access to reporting capabilities for daily operational analysis and long term strategic program effectiveness.
2) System limitations restrict reporting capabilities to provide accurate trending analysis to proactively reduce preventable mishaps in all classes.
3) Limited availability of authoritative information regarding Safety Program Management (SPM) data and all Classes of mishaps, near-misses, and hazards, across the Navy and Marine Corps enterprise, commands, programs and Communities of Interest (COIs).[32]

In addition, the analysis provides 18 conditions contributing to problems with their current systems resulting from a lack of focus on proactive mishap prevention capabilities to the inability to conduct advanced analytics with their systems.[33]

The Navy's "To-Be" analysis highlights four primary High Level Outcomes for the RMI:

1) Improved resource utilization for SOH programs and initiatives.
2) Enterprise-wide SOH trend identification to identify risks and improvements.
3) Advanced analytics capabilities to determine deep seated mishap causalities and mitigation.
4) A single enterprise safety environment in support of Analysis and Dissemination (A&D) processes at all levels of the DON enterprise.[34]

Nowhere within the analysis is there mention of potential interoperability with the other services, cost savings projections, or of planned utilization of cloud technologies to support the new system. The expected cost for this project across the first year of development is $7.1M with an estimated Future Year Defense Program (FYDP) requirement of approximately $35M.[35]

In contrast, the AFSAS program, initiated in 2003 and formally stood up in 2007, cost the AF $6.5M over five years; approximately $1.3M per annum. Total cost of the AFSAS program

(2003-2014): $18M, or $1.68M per annum.[36] This significant difference, as compared with the Navy's proposal, is attributed primarily to efficient in-house development and programming efforts at AFSEC.

Beyond the basic cost comparison, the AFSAS program has steadily increased capability due to a robust and tightly controlled requirements gathering and development process instituted by AFSEC for the program. Mr. James Johnson, AFSEC CIO and Division Chief of the Analysis and Integration Division states, "I believe we have the best requirements gathering, and requirements development process in the DOD…we are successful because we have one person in charge of the requirements team, who is credible with both the functional and IT experts driving software development efforts for AFSAS. By having this organization, we ensure field-level concerns and requirements are addressed, and development strategies and decisions are prioritized and implemented with minimal delays."[37] Since 2007, AFSAS has been the single, one-stop, safety data system for the AF across all disciplines. It has streamlined reporting and incorporated new capabilities such as a comprehensive data extraction toolset, an occupational-illness reporting module, file attachment capabilities, and comprehensive user administration functions. In addition, a myriad of capabilities such as mishap report quality control functions, business intelligence tools for interactive analysis, charting, and report building, motorcycle safety training and tracking functions, as well as oversight of mishap investigations from preliminary message to final release (to include all required investigation Tabs and associated information) are built into the current functionality of AFSAS.

In addition, to its diverse functionality, AFSAS is considered by Mr. Frank Kendall, Under Secretary of Defense Acquisition, Technology and Logistics (OSD/AT&L) to be, "…a highly capable safety reporting/trending system."[38] From the Macro-comparisons, AFSAS is the

clear leader in overall functionality, cross-discipline scalability, as well as extensive data extraction and analysis capability. AFSAS is positioned to serve as the single safety reporting system for DOD and already hosts several outside agencies. To date, the Defense Contract Management Agency (DCMA), Defense Commissary Agency (DeCA), Defense Intelligence Agency (DIA) (Aviation), and the Combatant Commands (COCOMS) utilize AFSAS for all their safety reporting requirements and OSHA by-law reporting requirements.[39] Additionally, AFSAS is the first and only service safety system, with level-3 data security requirements, to be approved for operation on a commercial cloud system as directed under the "Cloud First" policy. This move saves the AF $3.0M+ over a three year period by leasing the commercial cloud servers versus hosting them locally.[40] AFSEC projected costs to maintain an organic AFSAS server-farm capability at $1.5M-$2.0M over a three year period for replacement and sustainment costs. In addition, cost comparisons of the DOD Defense Information Systems Agency (DISA) Cloud services versus Amazon Cloud Services showed a huge disparity. DISA projected annual Cloud service hosting costs at $1.2M, with a $400K set-up fee, while Amazon projected out at $200K-$240K annually.[41] Due to the cost savings, AFSEC elected to pursue the commercial Cloud option, gained required Authority to Operate (ATO), successfully migrated to the Amazon Cloud, and began seamless Cloud operations of AFSAS on 28 March 2014.[42]

CONCLUSIONS

In today's fiscal environment of ongoing manpower and funding cuts, it is essential for DOD and military leaders to carefully consider where consolidation and leveraging of resources can be made. As discussed, the why, what, and how of mishap data collection is nearly identical across the services, but there is little standardization amongst the safety data systems employed by the services and DOD. Implementation of a joint-service safety data system will help meet the

challenges of future development strategies and support the concepts and direction of the Goldwater-Nichols act by reducing duplication of effort, directly support the FDDCI vision for cost reductions of data center hardware, software, and operations, and help implement the DOD IT Enterprise Strategy Roadmap for aggressive IT consolidation, as well as leverage the benefits of Cloud migration and hosting to improve IT flexibility, responsiveness, and overall costs to the services and DOD.

Although each service provides the required capabilities to capture mishap, injury, occupational illness, and hazard data, AFSAS is the only system combining the disciplines within a single, one-stop data system. In addition, the AFSAS requirements and development team has successfully scaled the system to incorporate outside agencies, their specific requirements, and data sets within the current operating budget of the AFSAS program. Continuous process improvement, and cost effectiveness strategies, are evident in AFSEC's module development efforts, as well as its migration to the commercial Cloud; a first in DOD for this level-3 data security system, and a benchmark for other programs to follow. In addition, its ad-hoc query and business intelligence tools provide users with effective analysis tools, graphing, and report generation capabilities exceeding all other current service systems.

To fully exploit the benefits of AFSAS as the joint-service safety data system, the following recommendations are offered:

- **First recommendation:** Create a joint program office to oversee the joint-service safety data-collection system and leverage joint-service personnel and funding to support development and quality control requirements for migration of required data from these agencies into the joint system.
- **Second recommendation:** Build comprehensive requirements and functionality into the joint-system to accommodate the data sets and unique differences of the included DOD components and agencies.
- **Third recommendation:** Develop service team leads to train appropriate personnel with the system prior to use.

- **<u>Fourth recommendation</u>:** Continue to develop capabilities, and streamline functionality as necessary to meet future DOD component and agency needs.

Effective hazard identification and proactive mishap prevention are essential for saving lives and preserving future combat capability. Ensuring timely safety data collection, trending and analysis capabilities for the DOD components is essential to supporting these efforts. AFSAS is scalable, cost effective, and provides these needed capabilities today. With the proper resourcing and support it will be the premiere joint-safety data system of the future.

Notes

1. On-duty operations, training, as well as support activities across the functional areas of the military (Afloat, Aviation, Ground [Ashore], Motor Vehicle, Space, and Weapons), combined with off-duty activities of service members, account for the majority of hazards/mishaps experienced by the DOD and its service members. Consequently, mishap data is reported, collected, and analyzed for hazard/mishap mitigation/prevention under these same functional categories.

2. Air Force Safety Center, AFSEC/SEA Division, "USAF Safety Perspective" (presentation, Air Force Safety Center, NM for ANG Conference Brief, September 2008), Slide 4.

3. Ibid., Slide 5.

4. Department of Defense Instruction (DODI) 6055.07, *Mishap Notification, Investigation, Reporting and Record Keeping*, 6 June 2011, 1.

5. Ibid., 2.

6. Ibid., 36.

7. Air Force Instruction (AFI) 91-204, Safety Investigations and Reports, 10 April 2014, 21; Army Regulation (AR) 385-10, The Army Safety Program, 27 November 2013, 26; Commandant Instruction (COMDTINST) M5100.47A, Safety and Environmental Health Manual, August 2014, 318.

8. Ibid., 28.

9. Ibid., 29-31.

10. Ibid., 28.

11. Department of Defense, *DOD HFACS, Department of Defense Human Factors Analysis and Classification System Guide*, 11 January 2005; MOU signed by the following service Safety Chiefs: MGen McFann (USAF), Chief AF Safety; BGen Smith (USA), Director of Army Safety; RADM Brooks (USN), Commander Naval Safety Center; RADM Higgins (USCG), Director of Health and Safety U.S. Coast Guard; Col Wenger III (USMC), Director of Safety, Memorandum of Agreement between the Army Combat Readiness Center, Naval Safety Center, Headquarters United States Marine Corps (Safety Division), United States Coast Guard Health and Safety Directorate, and Air Force Safety Center, 11 January 2005.

12. DOD Safety Information Management Working Group, *Appendix B1, Data Definitions*, (2008); https://www.denix.osd.mil/denix_secure/loader.cfm?csModule=security/getfile&pageid=36410, (accessed 26 November 2014).

13. Ibid.

14. Risk management (RM), safety inspection programs, hazard abatement/reporting programs and tools help identify hazards, and contribute to the safety, risk awareness include: the Aviation Safety Action Program (ASAP), Military Flight Operations Quality Assurance (MFOQA), Line Operations Safety Audits (LOSA), Organizational Safety Assessment (OSA), Air Force Combined Mishap Reduction System (AFCMRS), Fatigue Avoidance Scheduling Tool (FAST), Ground Risk Assessment Tool (GRAT), Travel Risk Planning System (TRiPS), etc.). Specifics on these programs can be found on the service safety center websites or by contacting the service safety centers for additional information.

15. AFI 91-204, Chapter 5; AR 385-10, Chapter 3; Chief of Naval Operations Instruction (OPNAVINST) 5102.1D, Navy & Marine Corps Mishap and Safety Investigation, Reporting and Record Keeping Manual; 7 January 2005, Chapters 3-5; Chief of Naval Operations Instruction (OPNAVINST) 3750.6S, Naval Aviation Safety Management System, 13 May 2014, Chapters 4-8; Commandant Instruction (COMDTINST) M5100.47A, Chapter 3.

16. As directed in DODI 8500.01, DODI 8502.02, and DODI 8510.01, and with all other DOD, Federal Information Security Management Act, Federal Risk and Authorization Management Program (FedRAMP), and service-specific security protocols/ procedures required to operate these systems on standard government and/or commercial cloud networks. Specific references annotated in endnotes 23-27; Department of Defense Instruction (DODI) 8500.01, Cybersecurity, 14 March 2014; Department of Defense Instruction (DODI) 8502.02, Public Key Infrastructure (PKI) and Public Key (PK) enabling, 24 May 2011; Department of Defense Instruction (DODI) DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), 12 March 2014; E-Government Act of 2002, Title III-Information Security (Federal Information Security Act of 2002).Public Law 107-347. 107th Cong, 17 December 2002; FedRAMP Agency Site, Secure Your Cloud, Web resource, http://cloud.cio.gov/action/secure-your-cloud (accessed 15 Nov 2104).

17. U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Reporting & investigation tab; U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Reporting & investigation tab/Ground Accident Forms, https://safety.army.mil/REPORTINGINVESTIGATION /Forms/ GroundAccidentForms.aspx, (accessed 27 November 2014); U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Reporting & investigation tab/Aviation Accident Forms https://safety.army.mil/REPORTINGINVESTIGATION/Forms/AviationAccidentForms.aspx, (accessed 27 November 2014).

18. U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), *Risk Management Information System Webpage*, https://rmis.safety.army.mil/Login.aspx?ReturnUrl=%2fPages%2fHome.aspx, (accessed 27 November 2104).

19. U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), ReporIt Information Center-Benefits, https://reportit.safety.army.mil/InfoCenter/Information.aspx?t=5, (accessed 27 November 2014).

20. AFSEC-Air Force Safety Center, Forms webpage, https://www.my.af.mil/gcss-af/USAF/ep/browse.do?categoryId=pF575FC8E240BBA870124A1C76CC120A3&channelPageId=s6925EC13537F0FB5E044080020E329A9, available AF mishap reporting forms include: AF IMT 711B, *USAF Mishap Report*; AF IMT 711C, *Aircraft/UAV Maintenance Material Report*; and AF IMT 711D, *Nuclear Mishap/Incident Report*; (accessed 27 November 2014); Air Force e-Publishing website, http://www.e-publishing.af.mil/, available mishap reporting AF Forms AF IMT 711B, *USAF Mishap Report*; AF IMT 711C, *Aircraft/UAV Maintenance Material Report*; and AF IMT 711D, *Nuclear Mishap/Incident Report*; AF Form 190, *Occupational Illness/Injury Report*, and AF Form 978, *Supervisory Mishap Report*, (accessed 27 November 2014).

21. Chief of Naval Operations Instruction (OPNAVINST) 3750.6S, 4-1.

22. Chief of Naval Operations Instruction (OPNAVINST) 5102.1D, 5-1, 5-10 through 13.

23. Donald "Deke" Forbes, Senior Systems Analyst, FR2 Support Team, to the author, e-mail, 2 November 2014

24. *Goldwater-Nichols Department of Defense Reorganization Act of 1986.* Public Law 99-433. 99th Cong., 1 October 1986, Sec 153, Report on Assignment of Roles and Missions.

25. Vivek Kundra, U.S. Chief Information Officer, Office of Management and Budget, memorandum to Chief Information Officers, 26 February 2010.

26. Ibid.

27. Department of Defense, *Department of Defense (DOD) Information Technology (IT) Enterprise Strategy and Roadmap*, Version 1.0, 6 September 2011, iv.

28. Ibid.

29. Vivek Kundra, U.S. Chief Information Officer, Office of Management and Budget, *Federal Cloud Computing Strategy*, 8 February 2011, 2.

30. Naval Safety Center, *Risk Management Information (RMI): Analysis and Dissemination (A&D) Problem Statement*, Version 1.0, 28 April 2014,

31. Ibid., 4.

32. Ibid., 7.

33. Ibid., 4-5.

34. Ibid., 1.

35. Ibid., 23.

36. Dennis Christensen, AFSAS Program Manager, Air Force Safety Center, *Air Force Safety Automated System (AFSAS)*, bullet background paper, 17 November 2011; James Johnson, (AF Safety Center CIO/Analysis and Integration Division Chief), interview by author, 6 November 2014.

37. Ibid.

38. James Johnson and Michael Collins, AFSAS CIO & Deputy Division Chief, Analysis and Integration Division, *Air Force Safety Automated System Budget Cuts*, bullet background paper, 19 May 2014.

39. Ibid.

40. Ibid.

41. Mike Collins, Deputy Division Chief, Analysis and Integration Division, Air Force Automated System (AFSAS) Residing on Commercial Cloud Service, Point Paper, 24 January 2014.

42. Air Force Safety Center, *Air Force Safety Automated System Cloud Migration Implementation Process and Lessons Learned*, White Paper, 20 June 2014, 15.

Bibliography

Army Regulation (AR) 385-10, *The Army Safety Program*, 27 November 2013.

Air Force Instruction (AFI) 91-204, *Safety Investigations and Reports*, 10 April 2014.

Air Force Safety Center, AFSEC/SEA Division, "USAF Safety Perspective" (presentation, Air Force Safety Center, NM for ANG Conference Brief, September 2008).

Air Force Safety Center, *Air Force Safety Automated System Cloud Migration Implementation Process and Lessons Learned*, White Paper, 20 June 2014.

Chief of Naval Operations Instruction (OPNAVINST) 5102.1D, *Navy & Marine Corps Mishap and Safety Investigation, Reporting and Record Keeping Manual*; 7 January 2005.

Chief of Naval Operations Instruction (OPNAVINST) 3750.6S, *Naval Aviation Safety Management* System, 13 May 2014.

Commandant Instruction (COMDTINST) M5100.47A, *Safety and Environmental Health Manual*, August 2014.

Department of Defense Instruction (DODI) 6055.07, *Mishap Notification, Investigation, Reporting and Record Keeping*, 6 June 2011.

Department of Defense Instruction (DODI) 8500.01, *Cybersecurity*, 14 March 2014.

Department of Defense Instruction (DODI) 8502.02, *Public Key Infrastructure (PKI) and Public Key (PK) enabling*, 24 May 2011.

Department of Defense Instruction (DODI) DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, 12 March 2014.

Department of Defense, *DOD HFACS, Department of Defense Human Factors Analysis and Classification System Guide*, 11 January 2005

DOD Safety Information Management Working Group, *Appendix B1, Data Definitions*, (2008); https://www.denix.osd.mil/denix_secure/loader.cfm?csModule=security/getfile &pageid=36410 (accessed 26 November 2014).

Dennis Christensen, AFSAS Program Manager, Air Force Safety Center, *Air Force Safety Automated System (AFSAS)*, bullet background paper, 17 November 2011.

Donald "Deke" Forbes, Senior Systems Analyst, FR2 Support Team, to the author, e-mail, 2 November 2014.

Department of Defense, *Department of Defense (DOD) Information Technology (IT) Enterprise Strategy and Roadmap*, Version 1.0, 6 September 2011.

*E-Government Act of 2002, Title III-Information Security (Federal Information Security Act of 2002).*Public Law 107-347. 107th Cong, 17 December 2002.

FedRAMP Agency Site, *Secure Your Cloud*, Web resource, http://cloud.cio.gov/action/secure-your-cloud, (accessed 15 November 2104).

Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433. 99th Cong., 1 October 1986.

James Johnson, (AF Safety Center CIO/Analysis and Integration Division Chief), interview by author, 6 November 2014.

James Johnson and Michael Collins, AFSAS CIO & Deputy Division Chief, Analysis and Integration Division, *Air Force Safety Automated System Budget Cuts*, bullet background paper, 19 May 2014.

MGen McFann (USAF), Chief AF Safety; BGen Smith (USA), Director of Army Safety; RADM Brooks (USN), Commander Naval Safety Center; RADM Higgins (USCG), Director of Health and Safety U.S. Coast Guard; Col Wenger III (USMC), Director of Safety, Memorandum of Agreement between the Army Combat Readiness Center, Naval Safety Center, Headquarters United States Marine Corps (Safety Division), United States Coast Guard Health and Safety Directorate, and Air Force Safety Center, 11 January 2005.

Mike Collins, Deputy Division Chief, Analysis and Integration Division, Air Force Automated System (AFSAS) Residing on Commercial Cloud Service, Point Paper, 24 January 2014.
Naval Safety Center, *Risk Management Information (RMI): Analysis and Dissemination (A&D) Problem Statement*, Version 1.0, 28 April 2014.

U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Reporting & investigation tab/Aviation Accident Forms https://safety.army.mil/ REPORTINGINVESTIGATION/Forms/ AviationAccidentForms.aspx (accessed 27 November 2014).

U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Reporting & investigation tab/Ground Accident Forms, https://safety.army.mil/ REPORTINGINVESTIGATION/Forms/ GroundAccidentForms.aspx (accessed 27 November 2014).

U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), Risk Management Information System Webpage, https://rmis.safety.army.mil/Login.aspx?ReturnUrl=%2fPages %2fHome.aspx (accessed 27 November 2104).

U.S. Army Combat Readiness/Safety Center (USACR/Safety Center), ReporIt Information Center-Benefits, https://reportit.safety.army.mil/InfoCenter/Information.aspx?t=5 (accessed 27 November 2104).

Vivek Kundra, U.S. Chief Information Officer, Office of Management and Budget, memorandum to Chief Information Officers, 26 February 2010.

Vivek Kundra, U.S. Chief Information Officer, Office of Management and Budget, *Federal Cloud Computing Strategy*, 8 February 2011.