# Overview of Draft MIL-STD-882D w/CHANGE 1

**NDIA Systems Engineering Conference**
**Track 5 - System Safety - ESOH**
**San Diego, CA**

**Robert E. Smith, CSP**
**Booz Allen Hamilton**

**Sherman G. Forbes**
**U.S. Air Force**

**October 28, 2009**

# Bottom Line Up Front (BLUF)

- MIL-STD-882D w/CHANGE 1, intended to
  - Be evolutionary, not revolutionary, change
  - Build on Acquisition policy advances since 2004
  - Improve standardization
  - Increase inclusion of health and environmental risk management
  - Emphasize integration into Systems Engineering
  - Support implementation of 8 Dec 08 DoDI 5000.02

# Overview

- MIL-STD-882D – Overview and Problem
- DoD Policy and Guidance – The Response
- Drivers to Revise 882D
- Key Tenets in Revision Process
- Review of the Changes

# MIL-STD-882D Overview

- MIL-STD-882D - Feb 2000
  - Converted to a performance-based standard practice
    - Required by the Military Specifications and Standards Report (MSSR) initiative to retain 882
    - Defined what is required, not how to
    - Task descriptions removed
  - Enabled Program Offices to put 882D on contract without approval
  - Government and Industry recognized need for creation of supporting guidance on how to effectively utilize

# MIL-STD-882D – The Problem

- Neither Government or Industry provided the required support
- Confusion existed on lack of need for approval to require 882D
- No DoD Acquisition policy requirement to utilize 882D
- 12 May 03 DoDI 5000.2, Operation of the Defense Acquisition System, had limited and confusing guidance on safety, health, and environment risk management
- Perception and reality that DoD Acquisition policies and guidance did not support robust System Safety requirements
- Both System Safety and MIL-STD-882D atrophied

# DoD Policy and Guidance – The Response

- 19 May 03 Secretary of Defense (SECDEF) policy memo "Reducing Preventable Accidents," 19 May 2003
- Sep 03 Defense Safety Oversight Council (DSOC) created to direct responses across DoD to SECDEF memo
  - DSOC originally established ten Task Forces to focus on variety of areas of mishap prevention
    - From aviation safety to deployments and operations
    - Acquisition and Technology Programs Task Force (ATP TF)
      - Stood up in January 2004
      - Chaired by office of the Undersecretary of Defense (Acquisition, Technology, and Logistics), Deputy Undersecretary of Defense (Acquisition and Technology), Director of Systems and Software Engineering

# DoD Policy and Guidance – The Response

- ATP TF teamed with DoD Acquisition Environment, Safety, and Occupational Health (ESOH) IPT to integrate ESOH risk management into Systems Engineering using the DoD Standard Practice for System Safety, MIL-STD-882D
  - Developed a series of policy initiatives and implementation guidance to support that objective
- 23 Sep 04 AT&L memo "Defense Acquisition System Safety"
  - Specifically mandated use of MIL-STD-882D to manage ESOH risk as part of the Systems Engineering process
  - Requires Program Managers to report ESOH risk status and acceptance decisions at technical and program reviews

# DoD Policy and Guidance – The Response

- Apr 05 Defense Acquisition University course CLE009, "System Safety in Systems Engineering"
  - First formal guidance on how to use MIL-STD-882D
  - Should have been developed in 2000 (along with other more detailed System Safety analysis guidance)
  - Mapped the 882D System Safety processes into the overall DoD Systems Engineering processes using the DoD SE Vee model
  - Vetted by environmental engineers, industrial hygienists, System Safety engineers, and Systems Engineers
  - Over 2000 personnel have now taken this course

# DoD Policy and Guidance – The Response

- Nov 06 Defense Acquisition Guidebook
  - Much more detailed guidance on ESOH risk management
    - Using MIL-STD-882D
    - Integrating ESOH risk management into Systems Engineering
  - Explicitly mandated use of MIL-STD-882D
  - Moved ESOH guidance into Systems Engineering
  - Clearly delineated the overlapping areas between ESOH and Human Systems Integration (HSI)
  - Described the topics that the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) must address

# DoD Policy and Guidance – The Response

- 21 Nov 06 AT&L memo “Reducing Preventable Accidents”
  - Required Program Managers at all program reviews to address
    - Status of each High and Serious ESOH risk
    - Compliance with applicable safety technology requirements
  - Included Program Offices in preparation of mishap reports
    - Required Program Offices to make recommendations for materiel mitigation measures to reduce the likelihood of reoccurrence of mishap
    - Focused on eliminating human error

# DoD Policy and Guidance – The Response

- 7 Mar 07 AT&L memo “Defense Acquisition System Safety – ESOH Risk Acceptance”
  - Required formal acceptance of ESOH risks prior to exposing people, equipment, or the environment to a known system-related ESOH hazard
  - Mandated User Representative Formal Concurrence for High and Serious ESOH risk acceptance
- 8 Dec 08 DoDI 5000.02, "Operation of the Defense Acquisition System"
  - Incorporated all the ATP TF sponsored AT&L memos
  - Moved the ESOH discussion from HSI to Systems Engineering
  - Mandated use of MIL-STD-882D

# Drivers to Revise 882D

- Desire to bring back the Task Descriptions from MIL-STD-882C to make them readily available for call out in contract documents
- Need to align with current OSD Acquisition Systems Engineering policy changes
- Standardize terminology and basic process elements to facilitate utilization
- Expand task descriptions to incorporate DoD ESOH perspective
- Add new tasks based on CLE009
- Support DoD strategic plans and goals

# Key Tenets in Revision Process

- Retain performance-based, standard practice approach
- Minimize changes to those necessary to update the document and incorporate tasks
- Incorporate the tasks as optional, not mandatory
- Ensure each task is a separate and distinct activity
- Minimize transition from current version, to build on policy and implementation progress to date
- Ensure process usable by entire spectrum of DoD Acquisition programs
- Describe how to establish a collaborative ESOH effort using the System Safety process

# Key Tenets in Revision Process

- Add subtitle to emphasize that 882D is used for assessing risks associated with environment and occupational health, not just risks related to safety
  - "ESOH Risk Management Methodology for Systems Engineering"
- Emphasize that MIL-STD-882D defines a process that exists as a part of the overall Systems Engineering process to
  - Provide coordinated ESOH inputs into Systems Engineering to minimize the environmental “footprint” of the system and improve safety of personnel and the system itself

# Review of the Changes

- Update will not be a re-issuance, it will be a change revision, to retain 882D designation in DoD Acquisition policies
- Made the definitions, Section 3, mandatory to standardize terminology and to facilitate implementation of DoD ESOH risk acceptance policy
  - New and updated definitions
    - Emphasis on software safety related terminology
    - Emphasis on reducing confusion between Mishap, Hazard, and Risk
    - New or updated definitions include: Causal factor, Critical Safety Item, ESOH Technology Requirement, Environmental impact, Event risk, Hazard, Level of Rigor, Loss, Mishap, Mitigation measure, Risk, Safety-critical, Safety related, Safety Significant, Target risk, User, User representative *and more*

# Review of the Changes

- Section 4 only other mandatory section with its eight steps
  1. Document the system safety approach
  2. Identify hazards
  3. Assess risk
  4. Identify risk mitigation measures
  5. Reduce risk
  6. Verify risk reduction
  7. Accept risk
  8. Manage Life-Cycle Risk

# Review of the Changes

- Section 4 also
  - Emphasizes the identification and derivation of applicable ESOH technical requirements
  - Defines System Safety design order of precedence with five levels (vs. four levels in 882D) – added “Reduce risk through design alterations
- Risk assessment matrices and Software safety matrices (an addition of three tables) added to Section 4
  - Provide for a standard process for all developmental and sustaining engineering activities
  - May be tailored with formal approval in accordance with Component policy

# Review of the Changes

- Matrix descriptions updated
  - For severity,
    - Dollar value on losses increased for today's program dollars
    - Logarithmic progression applied
  - For probability
    - Additional guidance provided as notes to discuss use of quantitative or qualitative analysis and use of individual item or fleet/inventory
    - "Eliminated" level added

# Review of the Changes

- Changed Task 102 from System Safety Program Plan to System Safety Engineering Plan
  - Emphasizes that System Safety is not a stand alone program, but one of many efforts integral to the Systems Engineering effort
  - Combines previous System Safety Program Plan and System Safety Management Plan into one task
- Added Task 105 Hazard Tracking System to provide guidance for the basic required elements of a hazard tracking system
- Added Task 107 Hazardous Materials Management Plan (HMMP)
  - Provides guidance on basic elements of a HMMP
  - Based on a Single Process Initiative

# Review of the Changes

- Added Task 208 Functional Hazard Analysis to provide guidance for identifying and classifying the system functions and safety consequences of functional failures
- Added Task 209 Systems-of-Systems Integration and Interoperability Hazard Analysis to analyze the system within the context of it's systems-of-systems for emergent hazards not found in other hazard analyses
- Added Task 210 Environmental Hazard Analysis to support design development decision; support risk acceptance decisions for environmental hazards; provide the system specific data to support National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements

# Conclusion

- MIL-STD-882D w/CHANGE 1, intended to
  - Be evolutionary, not revolutionary, change
  - Build on Acquisition policy advances since 2004
  - Improve standardization
  - Increase inclusion of health and environmental risk management
  - Emphasize integration into Systems Engineering
  - Support implementation of 8 Dec 08 DoDI 5000.02

# Questions?

**Robert E. Smith, CSP**
**Booz Allen Hamilton**
**1550 Crystal Drive, Suite 1100**
**Arlington, VA 22202-4158**
**703-412-7661**
**smith_bob@bah.com**

# Back Ups

# MIL-STD-882 History[1]

- **MIL-STD-882 - July 1969**
  - **First DoD System Safety standard**
  - **System Safety became mandatory on all DoD-procured products and systems**
- **MIL-STD-882A - June 1977**
  - **Centered on the concept of risk acceptance as a criterion for System Safety programs**
  - **Established categories for frequency of occurrence**
  - **Combined with long-standing hazard severity categories**

***1 Clifton Ericson II, A Short History of System Safety, Journal of System Safety, May-June 2006.***

# MIL-STD-882 History[1]

- **MIL-STD-882B - 30 March 1984**
  - Continued evolution of detailed guidance in both engineering and management requirement
  - Added emphasis on facilities and off-the-shelf acquisition
  - Addressed software in some detail for the first time
- **MIL-STD-882B, Notice 1 - July 1987**
  - Expanded software tasks
- **MIL-STD-882C - Jan 1993**
  - Integrated the hazard and software System Safety efforts
  - Removed individual software tasks
  - Combined software and hardware tasks

# MIL-STD-882 History[1]

- **MIL-STD-882C, Notice 1 - Jan 1996**
  - **Corrected some errors and revised the Data Item Descriptions**
- **MIL-STD-882D - Feb 2000**
  - **Converted to a performance-based standard practice**
    - » **Required by the Military Specifications and Standards Report (MSSR) initiative to retain 882**
    - » **Defined what required, not how to**
    - » **Task descriptions removed**
  - **Enabled Program Offices to put 882D on contract without approval**
  - **Government and Industry recognized need for creation of supporting guidance on how to effectively utilize**