

# CRWS-BoK:

## Modernizing the Body of Knowledge through Cyber Resilience

Angela Lungu, CRWS-BoK Project Lead  
Madison Rudy, CRWS-BoK Lead Analyst  
Contract Support to Director, System Security Policy, Guidance, and Standards  
Office of the Under Secretary of Defense for Research & Engineering

Presentation  
NDIA conference  
October 2024

<https://crws-bok.org>  
<https://www.CTO.mil>  
✕ @DoDCTO





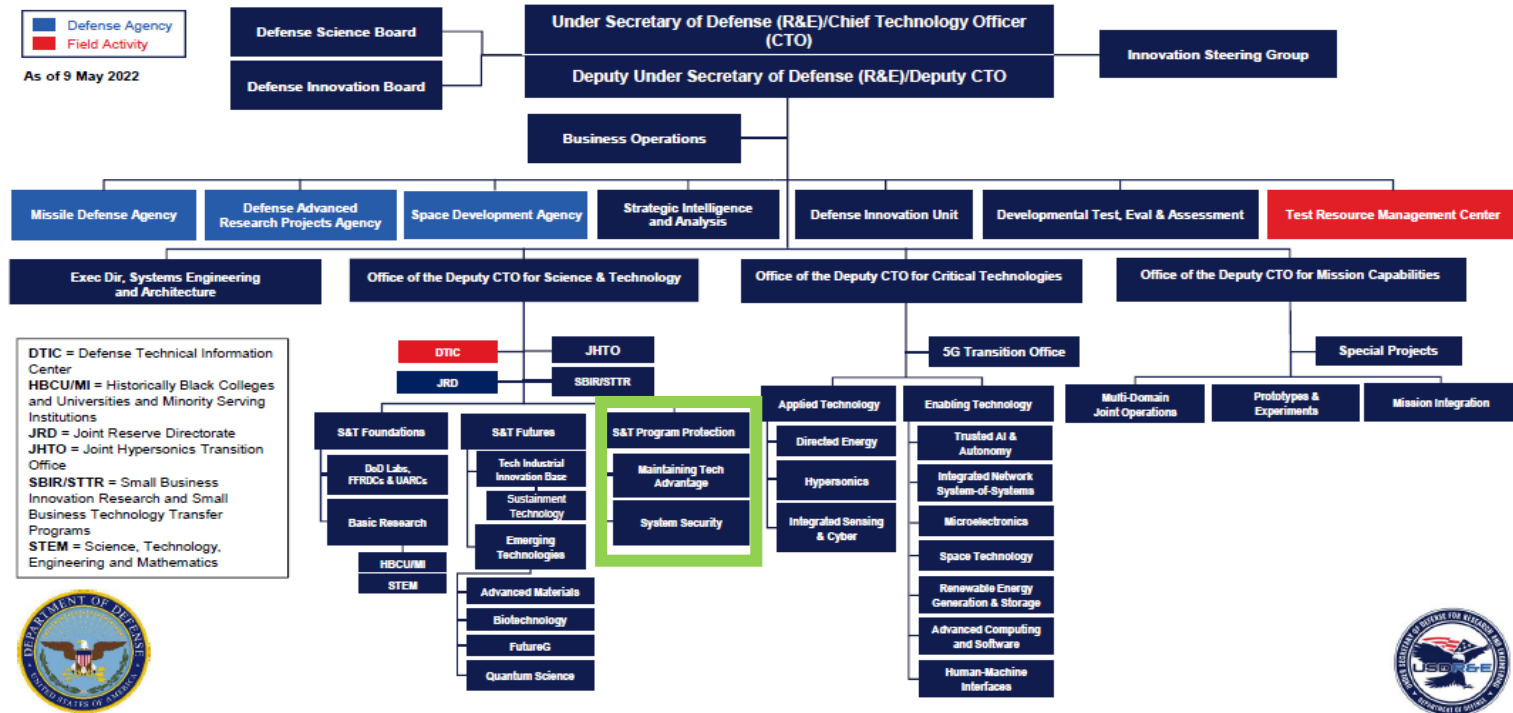
# Agenda

- Introduction
- General Overview
- Functionality Overview



# Introduction

## Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Organization



**STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through assured, secure and resilient systems and a healthy viable national security innovation base**



# Introduction

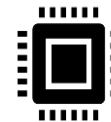
## System Security Mission and Priorities



### The Challenge

**Problem:** Adversary threats are outpacing policies and practices for engineering weapon systems; requires knowledgeable S&T and engineering workforce to provide dependably safe, secure, and resilient systems to operations at speed and scale

- Advance policy and guidance to balance technology and program protection that enables rapid delivery of warfighter capability
- **Strengthen System Security/Secure Cyber Resilient Engineering (SCRE) workforce through innovative education and training methods**
- Advance Technology and Program Protection methods to ensure technological superiority
- Advance the practice of Trust and Assurance through Joint Federated Assurance Center



### Lead Policy :

- DoDI 5000.83, DoDI 5200.44, DoDD 5200.47E

### Guidance:

- Program Protection Planning
- Information Communications Technology Supply Chain
- Secure Software Supply Chain
- Software Assurance
- Controlled Technical Information
- Hardware Assurance
- Anti-Tamper

### Standardization:

- Secure Cyber Resilient Engineering (SCRE)

### Competency:

- System Security Engineering (SSE)
- SCRE

ENGINEERING CYBER RESILIENT WEAPON SYSTEMS CRWS-BoK

Assurance Knowledge Management

Evidence-Based Assurance

Joint Federated Assurance Center (JFAC)

## System Security Mission: Foster Assured, Secure, Resilient Innovation, Missions, Systems and Components



# Introduction

**Comprehensive knowledge hub that not only provides easy access but also serves as an authoritative source of guidance and information with over 600 publicly available resources to support secure cyber resilience engineering activities**

***Visit us: <https://www.crws-bok.org>***

## Key Benefits

Easy and direct searches to quickly locate all your resources on one site

Regular updates to ensure the most current references are always available

Confidence of knowing your references come from credible resources

Highly curated and relevant content to make the most efficient use of your time

Developed for

- Science & Technology Managers
- Researchers
- Engineers

Across the **systems security engineering** & adjacent communities from

- Department of Defense
- Federal Government
- Industry
- Academia

First launched May 2021  
Version 4.2 released August 2024

## User Features

Receive free, unlimited access to all resources in CRWS-BoK

Save searches

Favorite resources

Annotate resources

Save resource annotations

Subscribe to email notifications when updates to resources and saved searches occur

Nominate resources for addition to the BoK

**A powerful repository and viewing environment that enables users to efficiently and easily access, search, annotate, save, and share the engineering information**



# General: Background

Initiated in 2019 as 2-year DAWDF prototype project

Initial policy & guidance gap analysis and framework development

Significant upfront effort spent developing and testing user interface

Access & outreach plans to reach desired user groups based on use case analysis

\* DAWDF (now DAWDA): Defense Acquisition Workforce Development Fund (Account)



# General: Repository Quality and Maintenance

## Maintaining Quality

**Users able to nominate new resources**

**Ongoing verification of resources for most current versions  
(or if superseded or rescinded)**

**User notification/related documentation when resource  
retired or rescinded**

**Algorithms & performance metrics leveraged to determine  
resource review schedule**

- How frequently accessed or if consistently rated not useful
- Poor performance places on “candidate for removal” list



# General: Repository Governance and Updates

## Adding Credible, Authoritative Content

- **Governance: Content Management Stakeholders from Government, industry and academia, with Curation Team facilitation**
- **Results: As of October 2024, 11 Review Boards have added 79 community-nominated resources to the repository**







# General: Top Challenges Facing S&T Professionals

After conducting usability testing interviews with industry and academia, the following challenges facing S&T professionals regarding engineering knowledge and resources were identified:



Figuring out if guidance & references are the most current versions

Determining if those references come from authoritative, credible sources



Difficulty wading through multiple sources and search engines to locate resources

Wasting time filtering and narrowing broad results in order to get to relevant information





# General: Value-Added CRWS-BoK Capabilities

CRWS-BoK meets those challenges and provides S&T professionals publicly available, authoritative guidance and knowledge to assist in the engineering of SCRE



Continuously updated resources to ensure users have most current versions

All resources are from credible, authoritative sources



Usability ratings & domain categories help users quickly and easily determine relative ratings and sources

All resources are conveniently located on one site

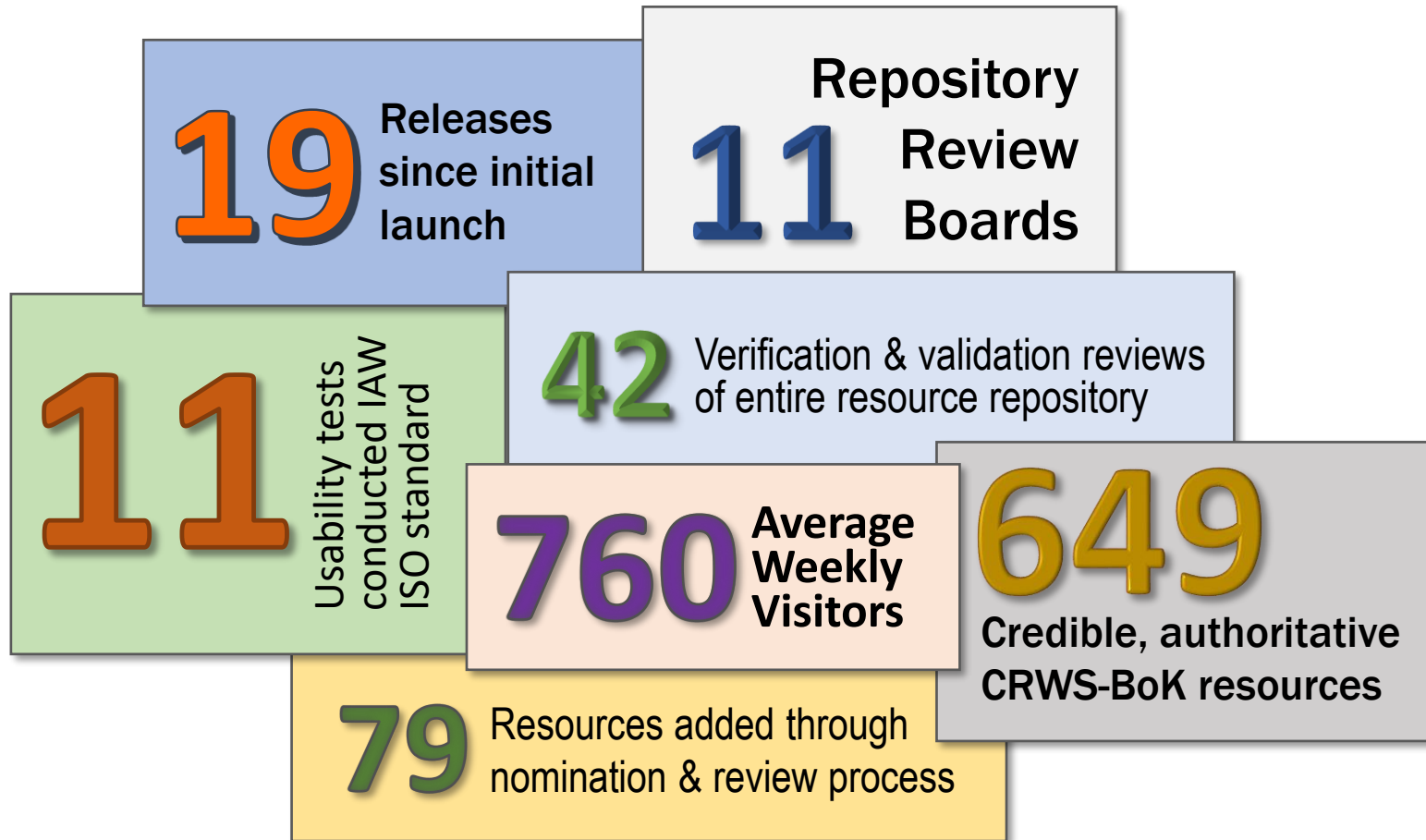


Highly curated resources supported by a review board process ensure focused, relevant repository content

*\* SCRE: Secure Cyber Resilient Engineering*



# General: CRWS-BoK by the Numbers



[As of Oct 2024]



# Functionality Overview

## Current Features

**Search**

- Guided search
- Keyword search
- Design Patterns
- Keyword filter
- Save a search
- Search w/i doc
- Defined filters

**General**

- Notifications
- Dynamic community metrics
- Streaming video
- List/Card views
- Help boxes
- Accessibility
- Site map
- Email support
- Dark mode

**Resources**

- Nominations
- PDF viewer
- PDF annotate
- Bookmark
- Download
- Print
- Share
- Favorite
- Details view
- Usability ratings
- User ratings
- Listed Page Count & File Size



# Functionality Overview

## Landing Page

The screenshot displays the CRWS-BoK landing page. At the top left is the CRWS-BoK logo. A search bar is located at the top center. Below the search bar is a navigation bar with a home icon, a settings icon, a help icon, and a sign-in link. A banner below the navigation bar reads: "Have a suggestion? Let us know! - Submit your feedback on what you think about CRWS-BoK, whether it helped you accomplish your task...".

The main content area is titled "Guided Search" and features a grid of hexagonal tiles representing different categories. The tiles include: Protection Categories, Interface, Functional, Configuration, Data, Processes, Design Development, Architecture Design, Risk Management, System Analysis, Requirements Management, Verification, Stakeholder Requirements, and a SEARCH button. The "Architecture Design" tile is highlighted in teal.

On the left side, there is a "Trending Resources" section with a dropdown menu set to "Most Popular" and a "Displaying: Last 7 Days" filter. Below this are several resource links: Concepts for Assurance Case..., Cyber Resiliency Framework..., System Security Engineering..., Defense Industrial Base Cybe..., Adequately Secure 1.0, Cybersecurity Design Patterns, Secure and Cyber Resilient E..., Interpreting "Cyber" 1.0, National Checklist Program fo..., and National Industrial Security Pr...

On the right side, there is a "News" section with the headline "CRWS-BoK v4.2 is here!". Below the headline is a list of features: Ability to enlarge the preview window, Page number preview (for Card View AND List View), File size preview is visible when hovering over download, Updated Card View layout; cards have been simplified with reduced number of icons for easier viewing, and Addition of hyperlinks in a resource's detailed view to quickly search & view other resources by the same authors or OPRs (similar to a wiki!). A "MORE..." button is located below the list.

Below the news section is a "Check Out the August Updates!" section with a list of updates: DoD Dictionary of Military and Associated Terms (external site) (updated 7/12/2024), 32 CFR Part 117 (National Industrial Security Program) (updated 8/2/2024), DFARS Clause 252.204-7012 (updated 7/29/2024), DFARS Subpart 208.14 (updated 7/29/2024), DAU Glossary (downloaded 8/12/2024), and DL-QCIC-81795 Software Quality Assurance Report (validation 8/8/2024).

At the bottom of the page, there is a "FEEDBACK" button and a "DISA" logo.



# Functionality Overview

## Save a Search/Search Notification

Email alert to registered user:

Save Search			
Name	Description	Notifications	Delete
DASD(SE) or USD(R&E) Supply Chain resources		DAILY	DELETE



# Functionality Overview

## Card Features

A Resource Card is a card-shaped representation of a resource, displayed with other cards as a group in the search result window. They contain the most essential data elements of each resource; similar to a book cover.

Purpose is to help inform user, allowing to sift through large numbers of resources in the most efficient manner possible

Adjust Date Range

1986 to 2024

APPLY

- ▶ Controlled Access (2)
- ▶ Topic (24)
- ▶ OPR Short (60)
- ▶ Resource Type (17)
- ▶ Domain (3)
- ▶ Copyright Details (2)
- ▶ Version Date (3)
- ▶ CSA (11)
- ▶ Abstraction Level (3)
- ▶ Loss Control Objective (4)
- ▶ User Rating Score (5)

**NIST SP 800-70**  
National Checklist Program For IT Products: Guidelines For Checklist...

Domains: National Institute of Standards and Technology

Usability Score: [Visual indicator]

OPR: National Institute of Standards and Technology

Version: 4

Version Date: 2/15/2018

Copyright: Public Domain

Rating: 4 stars (2)

Actions: [Icons for share, alert, download, etc.]

**DODI 5000.90**  
Cybersecurity For Acquisition Decision Authorities And Program...

Domains: [Icon]

Usability Score: [Visual indicator]

OPR: Under Secretary of Defense for Acquisition & Sustainment

Version: Original

Version Date: 12/31/2021

Copyright: Public Domain

Rating: 4 stars (1)

Actions: [Icons for share, alert, download, etc.]

**MP190668**  
Relationships Between Cyber Resiliency Constructs And Cyber...

Domains: [Icon]

Usability Score: [Visual indicator]

OPR: The MITRE Corporation

Version: Original

Version Date: 9/1/2019

Copyright: Third Party

Rating: 5 stars (3)

Actions: [Icons for share, alert, download, etc.]

**DI-SAFT-82080**  
Contractor's Safety Plan

Domains: [Icon]

Usability Score: [Visual indicator]

OPR: United States Department of the Navy

Version: [Text]

**CYBER RESILIENCY**  
System Security Engineering Cyber Guidebook

Domains: [Icon]

Usability Score: [Visual indicator]

OPR: United States Department of the Air Force

Version: [Text]



**MP190668**  
Relationships Between Cyber Resiliency Constructs And Cyber...

Domains: [Icon]

Usability Score: [Visual indicator]

OPR: The MITRE Corporation

Version: Original

Version Date: 9/1/2019

Copyright: Third Party

Rating: 5 stars (3)

Actions: [Icons for share, alert, download, etc.]

Registered Users:  
Additional Features

Proven method for knowledge workers to acquire and manage large amounts of data

Visual cues can be processed 60,000x faster than text\*

It only takes about .25 seconds to process and attach meaning to a symbol, while an average of 6 seconds to read 20-25 words\*

\* Visualteachingalliance.com



# Functionality Overview

## Card Features

**Full Resource Title & Shortened Title (when available)** → **DODI 5000.90**  
*Cybersecurity For Acquisition Decision Authorities And Program...*

**Type of resource**  
- Government (Directive or Non-Directive)  
- Non-Government/Industry → **Domains** (Gavel icon)

**Office of Prime Responsibility** → **OPR**  
Under Secretary of Defense for Acquisition & Sustainment

**Release Version & When the resource [update] was published** → **Version** Original  
→ **Version Date** 12/31/2021

**Copyright** Public Domain

**Internal algorithm to determine usability** → **Usability Score** 1

**Thumbnail of the resource** → [Thumbnail image]

**Page count** → 22

**User Rating** → 4 stars (1)

**Download & Share** → [Download and Share icons]





# Functionality Overview

## Search Results/List & Card Views

CRWS-BoK Search Results (Card View):

- Search: Functional Protection through Design Development
- Filters: Weapon Systems, Information Systems Security, Security Engineering, etc.
- Date Range: 2007 to 2024
- Buttons: CLEAR FILTERS, SAVE SEARCH, SHARE LINK, SORT BY, LIST VIEW (circled in green)
- Results (3 cards):
  - SCRE WHITE PAPER: System Reliability And How it Relates With Operations And Mission Assurance 1.0 (2)
  - SCRE WHITE PAPER: System Trustworthiness And Assurance 1.0 (2)
  - 21ST ANNUAL NATIONAL Defense Industrial Association Systems and Mission Engineering Conference: Leveraging System Safety to Improve System Security (1)

CRWS-BoK Search Results (List View):

- Search: Functional Protection through Design Development
- Filters: Weapon Systems, Information Systems Security, Security Engineering, etc.
- Date Range: 2007 to 2024
- Buttons: CLEAR FILTERS, SAVE SEARCH, SHARE LINK, SORT BY, CARD VIEW (circled in green)
- Results (List):
  - SCRE White Paper Series: System Assurance and How it Relates with Operations and Mission Assurance 1.0 (2)
  - SCRE White Paper Series: System Trustworthiness and Assurance 1.0 (2)
  - 21st Annual National Defense Industrial Association Systems and Mission Engineering Conference: Leveraging System Safety to Improve System Security (1)
  - DoDI 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems & Networks (TSN) (2)
  - Preparation Guide for the Joint Services Weapon Safety Review Safety Data Package (1)
  - Aircraft Survivability Journal: Summer 2023: Measuring the Wind: Determining a System's Cyber Combat Survivability Level (1)



# Functionality Overview

## Annotate & Save

NIST SP 800-70

### National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

Preview Details

RELATED ASSETS | BOOKMARK | DOWNLOAD | REPORT A PROBLEM

Autosave

NIST SP 800-70 REV. 4 NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS

#### Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

#### Abstract

A security configuration checklist is a document that contains **instructions or procedures for** configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.

#### Keywords

change detection; checklist; information security; National Checklist Program (NCP); security configuration checklist; Security Content Automation Protocol (SCAP); software configuration; vulnerability

(\*Registered User capability only)

Annotations are **auto-saved locally** to a registered users' account – only you will be able to see your annotations

Assurance is grounds for justified confidence that a claim has been or will be achieved [2]. Assurance is a function of the evidence's relevance, credibility, and accuracy and the ability to craft valid, logical, and compelling arguments to substantiate stated claims. Establishing assurance in achieving objectives increases certainty and reduces risk – risk may be viewed as an assurance deficiency. Assurance considerations are a significant factor in all [3].

The text advisory refers to a negative influence, specifically those conditions that can cause a loss of trust.

Significantly, "advisors" include subjective assessments. We have necessary in absence of certainty of the subjective assessments.

3

weapon system engineering activities. Weapon systems are a system class with an essential purpose to deliver initial force with the intent to cause damage, and to deliver that initial force only when needed, only when armed, and only to the extent needed.

The implication is that all aspects of weapon systems engineering, across all contributing specialties, must provide confidence about the possibility for loss to occur. Assurance in the engineering results from planning, execution, decision-making, and judgments that can withstand the scrutiny of subject matter experts (SMEs) and is convincing.

The idealized statement of weapon system assurance is generalized in the form of a top-level claim and supporting sub-claims (Figure 1). Assurance addresses potential loss associated with the system under normal circumstances, when subjected to intentional disruptive actions, events, and conditions, and when subjected to unintentional disruptive actions, events, and conditions.

#### Weapon System Assurance Goal

- Provides effective control to achieve the following
  - Exhibits only the intended authorized behavior
  - Produces only the intended authorized outcomes
  - Any loss that occurs is acceptable

#### System achieves acceptable balance in the ability to

- Prevent loss and associated effects from occurring
- Minimize the extent of a loss and associated effects that does occur

#### System is effective in providing the required protection capability despite intentional actions, events, and conditions

#### System is effective in providing the required protection capability despite unintentional actions, events, and conditions

Figure 1 – Idealized Claims for Weapon Systems

The weapon system assurance goal should be judged based on the level of confidence in the system's ability to protect itself against loss and the associated consequences across all forms of adversary. The demonstration of compliance, functional testing, adversarial penetration

Guest Aug 29, 5:32 PM "necessary evidence of trustworthiness"

Guest Aug 29, 5:34 PM "reflect the problem"

Guest Aug 29, 5:32 PM "can be verified as being satisfied by a solution"

Guest Aug 29, 5:33 PM "define the solution space"

Guest Aug 29, 5:33 PM "policies, constraints, and concerns associated with the system's ability to achieve authorized and...more"

Guest Aug 29, 5:33 PM "I can even make comments on a document and then share this with someone else."

Add reply



# Contacts

## Angela Maria Lungu

- Project Lead for CRWS-BoK  
Support to System Security
- [angela.m.lungu.ctr@mail.mil](mailto:angela.m.lungu.ctr@mail.mil)



## Madison Rudy

- Lead Analyst for CRWS-BoK
- Support to System Security
- [madison.a.rudy.ctr@mail.mil](mailto:madison.a.rudy.ctr@mail.mil)