

UNCLASSIFIED



**RANCHER GOVERNMENT SOLUTIONS (RGS)
HARVESTER GOVERNMENT
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW**

26 August 2026

Developed by RGS and DISA for the DoW

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.2 Authority	1
1.3 Vulnerability Severity Category Code Definitions	1
1.4 STIG Distribution	2
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer	2
2. ASSESSMENT CONSIDERATIONS.....	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....	5
3.1 Architecture Overview	5

LIST OF TABLES

Table 1-1: Vulnerability Severity Category Code Definitions 1

Table 3-1: Definitions 5

LIST OF FIGURES

	Page
Figure 3-1: HCI Architecture.....	6

1. INTRODUCTION

1.1 Executive Summary

The Rancher Government Solutions (RGS) Harvester Government Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of War (DoW) information systems. This document is meant for use in conjunction with other STIGs, such as Rancher Multi-Cluster Manager (MCM), Rancher Kubernetes Engine 2 (RKE2), and appropriate operating system STIGs.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoW systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoW and federal government's computing environments can obtain the applicable STIG from the DoW Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a common access card (CAC) that has DoW Certificates can obtain the STIG from <https://public.cyber.mil/>.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoW organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DoW. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DoW architecture.

1.8 Product Approval Disclaimer

STIGs provide configurable operational security guidance for products being used by the DoW. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and

authorization (A&A) under the DoW Risk Management Framework (RMF). DoW AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DoW policy and through RMF risk acceptance. Inputs into acquisition or preacquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW federal/DoW mandated standards.

2. ASSESSMENT CONSIDERATIONS

The deployment must be built upon a pre-hardened, STIG-compliant foundation. The entire infrastructure stack must adhere to the following mandatory baseline configurations:

- **Host Operating System:** SUSE Linux Enterprise Micro 5 (SLEM 5) must be fully aligned with the DISA General Purpose Operating System STIG applied to SLE Micro. The underlying physical nodes must run SLEM 5. It must run with an immutable, read-only root file system and FIPS 140-2/3 mode enabled at the kernel level. Standard, unhardened commercial Linux distributions are strictly prohibited.
- **Kubernetes Runtime:** RKE2 must be deployed and configured IAW the DISA RKE2 STIG. RKE2 is mandatory because it is specifically engineered for the government, containing built-in security profiles, FIPS-validated cryptographic modules, and automated CIS benchmark alignment.
- **Enterprise Controller:** Rancher MCM must be deployed and configured IAW the DISA Rancher MCM STIG. Centralized orchestration, access policies, and virtualization management must be governed solely by a STIG-compliant instance of Rancher MCM. This ensures that administrative access to Harvester is secured via approved enterprise Identity Providers (IdP) and multifactor authentication (MFA).

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Architecture Overview

Rancher Harvester for Government is an out-of-the-box Hyperconverged Infrastructure (HCI) solution designed specifically to meet security and operational demands of U.S. Government and military missions. Developed by RGS, this pre-hardened platform allows federal agencies to run legacy virtual machines (VMs) and modern containerized workloads side-by-side seamlessly under a single, unified Kubernetes-driven management plane. Its architecture is highly optimized to ensuring reliable performance in Denied, Disrupted, Intermittent, and Limited (DDIL) environments typical of forward-deployed operations.

Harvester represents a paradigm shift from traditional proprietary virtualization to a cloud-native, open-source model. The table below outlines the primary concepts and conventions.

Table 3-1: Definitions

Team/Concept	Definition and Operational Context
HCI	A software-defined IT infrastructure that unifies computing, storage, and networking into a single system. Harvester achieves this by collapsing the traditional IT stack onto bare-metal servers, reducing hardware footprint and administrative overhead.
Bare Metal	Physical computer hardware (servers) without an underlying proprietary operating system or legacy hypervisor (like VMware ESXi). Harvester installs directly onto Bare Metal to act as the primary hypervisor and operating system.
RKE2	The underlying government-grade Kubernetes distribution that powers Harvester. RKE2 is hardened by default, FIPS 140-2 enabled, and designed to pass DISA STIG compliance checks, making it approved for secure DoW and federal networks.
KubeVirt	The core virtualization API technology within Harvester. KubeVirt extends Kubernetes, allowing it to schedule, run, and manage traditional VMs side-by-side with containerized applications within the same environment.
Longhorn	The cloud-native, highly available distributed block storage system used natively by Harvester. It provides resilient, replicated persistent storage for both VMs and containers without requiring an expensive external storage area network (SAN).
Tactical Edge/DDIL	Refers to forward-deployed operational environments characterized as DDIL. Harvester for Government is explicitly engineered to operate autonomously in these disconnected, low-bandwidth scenarios without “phoning home.”
Rancher Government Carbide	The secure software supply chain service provided by RGS. It ensures all Harvester components, updates, and images are cryptographically signed, verified, and free of known vulnerabilities before deployment.

Team/Concept	Definition and Operational Context
STIGatron/Security Operator	Automated compliance tooling built into the RGS ecosystem that continuously scans and enforces DISA STIGs across the Harvester cluster.

Figure 3-1: HCI Architecture

