ChatGPT

Integrating SIPRNet, DARPA-sponsored networks and Platform One into the Mycosoft environment

Background

What SIPRNet and DARPA-sponsored networks represent

- **SIPRNet (Secret Internet Protocol Router Network)** is the U.S. DoD's secure network for handling information up to the **secret** classification. It is separate from the public Internet and non-classified DoD network (NIPRNet). Moving data between SIPRNet and lower classification networks requires *cross-domain solutions* (CDS) that enforce policy-based separation and content inspection. CDSs are integrated information-assurance systems that provide a controlled interface for restricting or allowing the transfer of information between different security domains [1].
- **DARPA networks** – historically the Advanced Research Projects Agency Network (ARPANET) – were early research networks that eventually evolved into today's Internet. DARPA continues to sponsor research testbeds, but these networks are not general-use operational networks. Connections to classified DARPA environments must follow similar cross-domain safeguards as SIPRNet.

Platform One basics

Platform One is the DoD's enterprise DevSecOps platform. It provides:

- **Iron Bank:** a curated container registry. Every image in Iron Bank is assessed, scanned daily for vulnerabilities, and accompanied by an Overall Risk Assessment (ORA) score and vulnerability reports [2]. Iron Bank supplies standardized evidence such as SBOMs and risk assessments to support security compliance [2].
- **Big Bang:** an infrastructure-as-code baseline that packages a DevSecOps toolchain into a pre-integrated stack. Big Bang embeds the DoD's DevSecOps reference design and can shorten Authority-to-Operate (ATO) timelines from years to **around 90 days** [3]. It provides trusted, open-source tools configured to meet DoD requirements and allows teams to modify components while maintaining a standard baseline [4]. The platform is open source and governed by the Big Bang Technical Oversight Committee (BBTOC) [5].
- **Party Bus/CollabTools/EdgeOps:** platform-as-a-service offerings for deploying applications across cloud or edge environments.

Platform One currently operates on the DoD's unclassified network (NIPRNet) at **Impact Levels 2 and 4** and is being replicated to higher classification levels. The Air Force announced plans to move parts of Iron Bank to the **secret (IL-5)** environment and eventually to **top secret (IL-6)** [6]. Moving containers from an unclassified to a classified network is straightforward for well-structured files but becomes more complex for unstructured/binary code, which requires cross-domain solutions to ensure unsafe content is filtered [7].

Cross-domain solutions (CDS)

Because SIPRNet and DARPA networks operate at higher classification levels, integrating them with unclassified systems requires approved cross-domain solutions.

- A CDS is an integrated hardware/software system providing a controlled interface to enable or restrict the transfer of information between security domains based on a predefined security policy [8]. CDSs enforce **information separation** and perform deep content inspection and filtering [9].
- DoD cross-domain solutions are regulated by the **NSA's National Cross Domain Strategy and Management Office (NCDSMO)**. They are evaluated under the NSA's **"Raise the Bar" (RTB)** security framework; only NSA-approved or DoD-approved CDS products are authorized for use on SIPRNet or other operational defense networks [10]. Accredited CDSs often include high-assurance guards (HAGs) and hardware-enforced isolation to prevent data spills [11].
- Cross-domain solutions handle transfers **high-to-low** (classified to unclassified) and **low-to-high** (unclassified to classified). Transfers use policy engines, data diodes and guards to ensure only authorized content moves between domains [12].

Integration considerations for Mycosoft

Because Mycosoft is building systems for military and intelligence customers, any integration with SIPRNet or DARPA-sponsored networks must preserve classification boundaries and comply with DoD accreditation requirements. The following subsections outline a high-level technical approach.

1. Segregated environments and deployment topology

1. **Separate enclaves per classification level** – Deploy Platform One components (Big Bang, Party Bus, etc.) in distinct enclaves matching the classification of the target network. For example:
2. **NIPRNet / IL-2/IL-4**: continue running Mycosoft's unclassified workloads and the initial Big Bang baseline on `sandbox.mycosoft.com` for development and testing.
3. **SIPRNet / IL-5**: deploy a mirror of Mycosoft's DevSecOps environment within a secure, accredited DoD hosting environment (e.g., Cloud Works). Platform One documentation notes that CloudWorks provides SIPR IL-5 hosting [13]. This enclave must use DoD-approved hardware and networks; direct internet connectivity is prohibited.

4. **Top secret / IL-6+ (if required)**: similar pattern, using accredited TS hosting (e.g., JWICS). Because Platform One is beginning to support TS levels, close coordination with DoD CIO and NCDSMO is required [6].

5. **Networking and identity isolation** – Each enclave should have its own identity provider (IdP) integrated with DoD's identity systems (e.g., SIPRNet PKI tokens) and network segmentation. Use zero-trust networking principles: all services authenticate/authorize every request; boundary firewalls restrict egress/incoming flows.

6. **Infrastructure as Code** – Use Big Bang's helm charts and infrastructure-as-code templates to replicate the same toolchain across classification levels. Parameterize cluster configurations (domain names, IP ranges, identity provider endpoints) so that the same baseline can be applied to

`sandbox.mycosoft.com` and to IL-5/IL-6 environments. This approach simplifies ATO documentation because the configuration is auditable.

2. Secure transfer of containers and artifacts

1. **Use Iron Bank as the authoritative registry** – For open-source dependencies and third-party images, rely on Iron Bank's assessed containers. Iron Bank provides ORA scores, vulnerability reports and SBOMs [2], which help Mycosoft make risk-based decisions. Mycosoft should also onboard its own applications into Iron Bank so that DoD consumers can run them without replicating scanning pipelines.

2. **Replicate the registry across domains** – To make Iron Bank containers available on SIPRNet, the Air Force is moving the registry to IL-5/IL-6 [6]. Mycosoft should coordinate with Platform One to ensure its containers are included in the IL-5 mirror. If Mycosoft must host its own registry within SIPRNet, it needs a cross-domain solution for transferring containers from the unclassified build environment to the SIPRNet environment. This process should look like:

3. **Preparation on unclassified side**: build container image using CI/CD pipeline; run vulnerability scans; generate SBOM and ORA metadata; sign the container.

4. **Cross-domain transfer**: use an approved *transfer solution* (e.g., an accredited HAG with container scanning capability). Only the signed, structured container tarball and metadata are sent across. The CDS inspects the tarball to ensure it contains only expected file types and no malicious binary; unstructured code may require manual review [7]. The CDS enforces size limits and supports one-way flow (unclassified → SIPRNet) to prevent exfiltration.

5. **Receiving side**: load the container into a registry inside SIPRNet; verify the signature; attach the Iron Bank-style nutrition label. Use Big Bang's pipeline to deploy the image into Kubernetes clusters.

6. **Automate but maintain manual review** – While Mycosoft wants to automate transfers, Platform One's leadership notes that automation of unstructured code transfers remains challenging and currently involves manual checks [7]. Plan for a hybrid approach: automate scanning and packaging, but route high-risk files through a manual approval queue.

3. Application architecture and data flow

1. **Design for offline operation** – Systems hosted on SIPRNet cannot call external APIs on the open internet. When Mycosoft integrates features that depend on external data (e.g., weather feeds), it must either:
2. Mirror those feeds via approved cross-domain bulk transfer into SIPRNet; or

3. Implement air-gapped functionality that works with pre-loaded data. For dynamic data, establish periodic high-to-low or low-to-high transfers via CDS with frequency determined by mission needs.

4. **Control flows between domains** – Determine which data flows are required. For example, intelligence data may need to flow from SIPRNet to NIPRNet after declassification; Mycosoft must implement a *downgrading* path via a CDS. Transfer solutions require content filters, virus scanning

and human review to ensure that only properly sanitized information is released [8]. Conversely, updates to Mycosoft applications (patches, vulnerability fixes) will flow from NIPRNet into SIPRNet. Use one-way data diodes where possible [12].

5. **Logging and auditing** – Maintain detailed audit logs of all cross-domain transfers. CDS systems generally produce audit trails; integrate these logs into Mycosoft's SIEM for compliance and security monitoring. Ensure logs are also replicated to the classification level where the event occurred.

4. Compliance and accreditation

1. **Follow DoD RMF and DoD DevSecOps reference designs** – Mycosoft is already working on compliance; integration with SIPRNet requires a formal Authority to Operate (ATO) at IL-5 or IL-6. The DoD DevSecOps reference design describes the lifecycle and supporting pillars of DevSecOps and emphasizes automated security testing and continuous monitoring [14]. Align your pipeline with these practices, which are embedded in Big Bang, to shorten accreditation timelines.

2. **Continuous ATO (cATO)** – DoD is moving toward continuous authorization where security posture is continuously assessed rather than evaluated every few years. Platform One is adopting cATO processes [15]. Mycosoft should instrument its pipelines with continuous vulnerability scanning, container signature verification, and real-time compliance dashboards to support cATO.

3. **Coordinate with NCDSMO and Program Management Offices (PMO)** – Because cross-domain solutions and classified network connections require government oversight, engage early with the NCDSMO and your sponsoring PMO. They will guide selection of approved CDS hardware/software and the accreditation process.

5. Testing on `sandbox.mycosoft.com`

- Use **sandbox.mycosoft.com** as a lower-classification staging environment to test Big Bang deployments and container builds. Validate that CI/CD pipelines produce Iron Bank-compliant containers (including SBOMs and vulnerability reports). Test cross-domain transfer processes by simulating a CDS (e.g., using a script that enforces file type and size restrictions) and performing manual review of unstructured code. Measure the time required to package, transfer, and deploy images in the SIPRNet mirror.
- Adopt **infrastructure-as-code** for sandbox and production environments. This allows the same configuration to be reused in the IL-5 environment, reducing drift and simplifying ATO documentation.

6. Additional considerations

1. **Network resilience and edge operations** – Platform One's **EdgeOps** is designed for disconnected and degraded environments. If Mycosoft applications need to run at the tactical edge, consider using EdgeOps to deploy containerized workloads to field devices that can periodically sync with higher-level clusters once connectivity is restored.

2. **DARPA-sponsored testbeds** – For DARPA projects, integration may involve experimental networks. These typically require isolation and separate ATOs. Work with DARPA program security officers to

understand classification and data-handling requirements. Use the same cross-domain patterns described above: separate enclaves, CDS-mediated transfer, and Big Bang infrastructure.

3. **Vendor selection** – When choosing CDS hardware/software, consider vendors approved under NSA's RTB program [10]. Evaluate whether hardware-enforced isolation (data diodes) or software-based guards are appropriate. Hardware solutions provide deterministic one-way transfer but may limit throughput; hybrid architectures combine both approaches [12].

Summary

Integrating Mycosoft's systems with SIPRNet and DARPA-sponsored networks while leveraging Platform One requires more than simply connecting networks; it demands building separate, accredited DevSecOps environments at each classification level and using government-approved cross-domain solutions to transfer software and data. Platform One's Big Bang and Iron Bank provide ready-made baselines and secure container registries that can be mirrored into secret and top-secret domains [3] [6]. Cross-domain solutions enforce information separation and allow policy-controlled transfers between domains [8] [12]. Mycosoft should adopt infrastructure-as-code practices, integrate continuous security testing, and coordinate with DoD authorities to achieve and maintain accreditation. Testing on `sandbox.mycosoft.com` will help refine pipelines before moving them to SIPRNet. Ultimately, success depends on treating classified environments as distinct ecosystems while leveraging Platform One's DevSecOps tooling to maintain consistent, secure software delivery across all security domains.

---

[1] [8] [11] Cross-domain solution - Wikipedia
https://en.wikipedia.org/wiki/Cross-domain_solution

[2] [3] [4] [5] Platform One
https://p1.dso.mil/iron-bank

[6] [7] [15] Air Force's Software Factory is Moving Iron Bank to Classified Levels | GovCIO Media & Research
https://govciomedia.com/air-forces-software-factory-is-moving-iron-bank-to-classified-levels-2/

[9] [10] [12] Cross Domain Solutions: DoD-Approved CDS, TACDS & Hardware Suppliers
https://www.defenseadvancement.com/suppliers/cross-domain-solutions/

[13] software.af.mil
https://software.af.mil/

[14] DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf