Secure Halo Advises Contractors to Keep NIST 800-171 Work Moving

October 28, 2026

SILVER SPRING, MD - October 28, 2026 -

Secure Halo, a cybersecurity advisory firm operating as a Mission Critical Partners company, is advising defense contractors to continue implementing NIST SP 800-171 controls while the Department of War's suspension of CMMC Phase 2 remains in place. The firm said the pause changed when third-party certification will be required, not the cybersecurity obligations contractors already carry under their contracts.

On July 13, 2026, the Department of War announced the immediate suspension of Cybersecurity Maturity Model Certification Phase 2 requirements, which had been scheduled to take effect on November 10, 2026. Phase 2 would have made third-party assessment a condition of award for many contracts involving controlled unclassified information. The department also suspended later CMMC implementation milestones and directed a CMMC Reform Task Force to conduct a 60-day review of the program. According to the department's announcement, all Phase 1 self-assessment requirements remain in place.

On September 3, 2026, the department issued Revision 3 of DFARS Class Deviation 2026-O0025, which carries the suspension into contracting guidance. Under the deviation, solicitations may include CMMC Level 1 and Level 2 self-assessments, and baseline compliance with NIST SP 800-171 Revision 2 under DFARS

clause 252.204-7012 remains required. Inside Government Contracts reported on September 21, 2026, that the Task Force report was due to the department's Chief Information Officer on September 11 but had not yet been made public.

Federal enforcement tied to the same controls has continued during the review. On September 1, 2026, the Department of Justice announced that Honeywell Aerospace Inc. agreed to pay $2,042,518 to resolve False Claims Act allegations that a business unit submitted claims for payment on a defense contract while failing to meet NIST SP 800-171 requirements on one network. The department noted that the claims are allegations only and that there has been no determination of liability. In June 2026, the department announced a $507,144 settlement with an Alabama defense contractor involving similar NIST SP 800-171 allegations.

Secure Halo said the combination of self-assessment and continued enforcement places more weight on the accuracy of what contractors report. During the suspension, a contractor's own assessment generally stands in place of independent certification, and the firm noted that such a representation can become the basis for a False Claims Act claim if the controls behind it are not actually in place. The firm is encouraging defense industrial base organizations to treat self-assessment scores and System Security Plans as statements that may need to be supported with evidence.

To support that work, Secure Halo is offering readiness assessments through its CMMC readiness services, which follow four phases aligned with NIST SP 800-171 and DFARS requirements. The program begins with scoping and a gap baseline that identifies where federal contract information and controlled unclassified information reside, then moves to a prioritized remediation roadmap, remediation of technical and procedural controls, and a pre-assessment validation. Deliverables include System Security Plan and Plan of Action and Milestones documentation, a control traceability and evidence map, and a mock assessment report.

The firm said organizations that continue this work during the pause may be better positioned for whatever the Department of War decides after the Task Force review. The program is available to prime contractors, subcontractors meeting DFARS flow-down requirements, suppliers and managed service providers that support controlled unclassified information environments, and emerging defense companies preparing for future bids.

"Paused is not the same as canceled, and contractors should not plan as if it were," said Matthew Yates, Director of Operations at Secure Halo. "The NIST SP 800-171 controls were in contracts before CMMC Phase 2 was ever scheduled, and they are still there today. What has changed is that a contractor's own assessment now carries more of the weight, so it needs to reflect what is actually in place. Organizations that keep moving on remediation now will have far less to make up if verification requirements return."

Secure Halo is an enterprise cyber risk and cybersecurity services firm based in Silver Spring, Maryland, operating as a Mission Critical Partners company. Founded in 2006, the firm joined Mission Critical Partners in 2022 and provides services spanning vCISO leadership, cybersecurity assessment, compliance management, managed detection and response, penetration testing, insider threat, and third-party risk management. It works with organizations across education, financial services, government, healthcare, insurance, manufacturing, public safety, and utilities, including federal contractors.

More information is available at Secure Halo.

###

For more information about Secure Halo, contact the company here:Secure HaloErin Webb202-629-1960info@securehalo.com962 Wayne Ave, Suite 310, Silver Spring, MD 20910


```
{
  "@context": "https://schema.org",
  "@type": "Organization",
  "name": "Secure Halo",
  "url": "https://securehalo.com/",
  "logo": "https://securehalo.com/wp-content/uploads/2025/01/securehalo-logo.png",
  "contactPoint": [
    {
      "@type": "ContactPoint",
      "telephone": "+1-202-629-1960",
      "contactType": "Customer Service",
      "email": "info@securehalo.com",
      "areaServed": "US"
    },
    {
      "@type": "ContactPoint",
      "telephone": "+1-301-304-1700",
      "contactType": "Sales",
      "email": "info@securehalo.com",
      "areaServed": "US"
    }
  ],
  "address": {
```

```
    "@type": "PostalAddress",
    "streetAddress": "962 Wayne Ave, Suite 310",
    "addressLocality": "Silver Spring",
    "addressRegion": "MD",
    "postalCode": "20910",
    "addressCountry": "US"
  },
  "sameAs": [
    "https://www.linkedin.com/company/secure-halo/",
    "https://twitter.com/SecureHalo",
    "https://www.facebook.com/SecureHalo",
    "https://www.youtube.com/@SecureHalo"
  ],
  "foundingDate": "2002-01-01",
  "founder": {
    "@type": "Person",
    "name": "Secure Halo Leadership Team"
  },
  "parentOrganization": {
    "@type": "Organization",
    "name": "Mission Critical Partners"
  },
    "description": "Secure Halo provides trusted, proactive cybersecurity solutions to protect organizations? data, infrastructure, and business continuity. With expertise across industries including government, healthcare, finance, manufacturing, and utilities, Secure Halo offers services such as vCISO, cybersecurity assessments, managed detection and response, compliance support, penetration testing, insider threat management, and third-party risk management."
}
```


Secure Halo

Secure Halo delivers trusted, proactive cybersecurity solutions?protecting data, infrastructure, and business continuity through services like vCISO, assessments, MDR, compliance, penetration testing, insider threat, and third-party risk management.

Website: https://www.securehalo.com/

Email: info@securehalo.com

Phone: 202-629-1960

