

Security Hack of F-35 Results in J-31. DOD Says NO MORE in Cybersecurity Enforcement Push



China's J-31's is ["modeled after"](#) the F-35. That is a nice way of referring to the [Chinese hack of F-35 data in 2007](#) through contractor Lockheed Martin, to build their jet fighter, J-31. Contractors are required to meet standards regarding security protocols but those requirements have not been verified in the past. Stacy Bostjanick, Direct of Cybersecurity Maturity Model Certification (CMMC) says that contractors in the past did not take the protocols seriously and simply [said they were complying in order to get business](#), resulting in the F-35 breach. Verification measures are needed because the voluntary compliance is resulting in too much mishandling of data.

["It's trust, but verify."](#) This is the start of a new day in the Department of Defense where cybersecurity, as we've been saying for years is foundational for acquisitions, we're putting our money where our mouth is. We mean it," explains Katie Arrington, CISO for the undersecretary of Defense for acquisition and sustainment.

The Pentagon will need to certify at least 1500 contractors and subcontractors as part of [fifteen contracts](#) ranging in size and complications, as a light rollout of the program. The CMMC will allow only a level 1 result, nothing below standard. The goal is to level the playing field for contractors that actually are complying with security standards because the Pentagon will not be able to accept cheaper contract options that are not in compliance. Some contractors have left vulnerabilities in place for years, even when simply security fixes were available.






There has never been a comprehensive, objective assessment conducted of the security posture of the US Defense Industrial Base of [over 300k companies](#).

"We have a great deal of standards for cybersecurity. What we are lacking is a unified standard. It is a major undertaking, but just like we got to ISO 9000, we need to get there with cybersecurity. If we were doing all the necessary security controls, we wouldn't be getting exfiltrated to the level that we are. We need to level set because a good portion of our defense industrial base doesn't have robust cyber hygiene. Only 1% of [Defense Industrial Base] companies have implemented all 110 controls from the National Institute of Standards and

Technology. We need to get to scale where the vast majority of DIB partners can defend themselves from nation state attacks.” explains CISO, Katie Arrington.

Federal agencies spend a greater percentage of their IT budgets on cybersecurity than many states

Federal agencies' cybersecurity budgets as a percentage of total IT budget and year-over-year growth

			2019	2020	2021
	Department of Transportation	Percentage of IT budget	5.63%	7.09%	7.33%
		Year-over-year increase	10.54%	21.12%	-4.92%
	Health and Human Services	Percentage of IT budget	6.44%	8.43%	8.12%
		Year-over-year increase	18.50%	-7.18%	9.19%
	Social Security Administration	Percentage of IT budget	11.40%	10.54%	10.79%
		Year-over-year increase	4.21%	1.76%	-1.25%
	Treasury	Percentage of IT budget	10.82%	11.77%	14.06%
		Year-over-year increase	-7.23%	15.19%	17.06%
	Justice	Percentage of IT budget	25.07%	30.07%	28.16%
		Year-over-year increase	-0.67%	7.56%	3.19%



Karen Heumann, G2M Communications, a re-grate-it brand