Security Without Governance is not Secure

Background

The Internet has quickly revolutionized the way governments, companies, and other organizations conduct business. But in their haste to gain market share and meet client/constituent expectations, many organizations are pushing out products and services that are not, and using IT infrastructure that is not, secure. This has made it easy for criminals and other adversaries to conduct ransomware attacks, steal data, manipulate systems, and even take control over critical infrastructure. These criminal acts are shutting down governments for weeks on end, forcing businesses out of business, and wreaking havoc on our national security and our economy. This needs to change.

> "*The United States faces **persistent and increasingly sophisticated malicious cyber campaigns** that threaten the public sector, the private sector, and ultimately the American people's security and privacy.*"
>
> President Biden, EO 14028

Throwing more technology at the problem is not the solution. We see this over and over again with organizations like the City of Baltimore, Equifax, Solar Winds, and others. These large organizations have large IT and cybersecurity budgets and numerous cybersecurity tools, yet they still suffer catastrophic breaches and crippling incidents. Root cause analyses of these incidents routinely shows that they are due to oversights that could have been remedied through proper governance.

Rather than expecting technology to solve the organization's problems, organizations must adapt to these new threats and embed security into their DNA. Until that happens, every organization is destined to remain at our adversaries' mercy.

DoD's Role in Creating National Cybersecurity Governance Awareness

No organization is more keenly aware of the need for this kind of change than the United States Department of Defense ("DoD"). DoD has watched as time and again our adversaries used weaknesses in DoD contractors' IT and cybersecurity programs to gain access to highly valuable information. From classified information such as planned troop movements to unclassified but still highly sensitive information like the design drawings for next-generation fighter jets and even seemingly mundane (but still highly valuable) equipment purchase information, our adversaries are aggressively hunting for any

and all of DoD's information. Our adversaries know they can weave these discrete threads of information into a rich tapestry that illustrates DoD's, and the broader government's, plans - and weaknesses. As a result, our adversaries can stand shoulder-to-shoulder with our warfighters, and even leapfrog ahead of them, without having to invest a dime in research and development.

DoD realized several years ago that this needs to stop. Contractors must be required to take cybersecurity more seriously and adopt more stringent requirements. DoD recognized that it needed to move cybersecurity from one of many contract-related factors and to instead make demonstrable cybersecurity a foundational requirement to do business with DOD.

> *"We **cannot** look at security and be willing to trade off to get lower cost, better performing products, or get something faster. If we do that, nothing works, and it will cost more in the long run."*
> Katie Arrington, CISO OUSD(A&S)

> *"In the end, the **trust** we place in our digital infrastructure should be proportional to how **trustworthy** and **transparent** that infrastructure is, and to the consequences we will incur if that trust is misplaced."*
> President Biden, EO 14028

CMMC

The result is DoD's Cybersecurity Maturity Model Certification ("CMMC") program. Under CMMC, contractors must not only attest that they are meeting requirements established by the National Institute of Standards and Technology ("NIST"), but they must also have an authorized third party certify that the contractor is meeting those requirements.

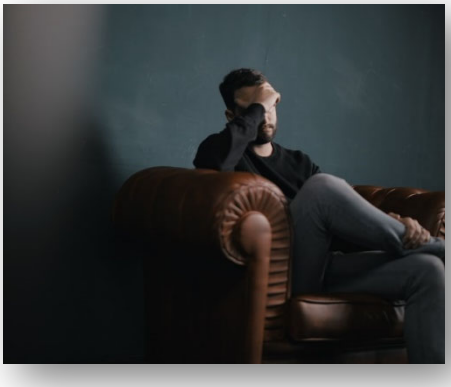
It is important to note that NIST's requirements aren't just limited to adopting certain technologies. Instead, they require a holistic rethinking of the organization's cybersecurity program, including ensuring that employees are well trained in cybersecurity, management is involved in cybersecurity planning, and, perhaps most importantly, that the organization understands the impact its own supply chain will have on the organization and DoD.

As a result of the CMMC program and related efforts, hundreds of thousands of companies across the nation, and even around the world, are being forced to pay more attention to their cybersecurity if they want to do business with the US government.

Even more importantly for our national and economic security, the supply chain analysis required by CMMC means that the government's program will have a ripple effect throughout the nation. Organizations, including those that do not work directly with DoD, will be looking to replace the weakest links in their supply chains to reduce the organization's own risk and the risks to their clients. As a result, more and more companies will be forced to embed cybersecurity into their own DNA.

The Problem for Contractors

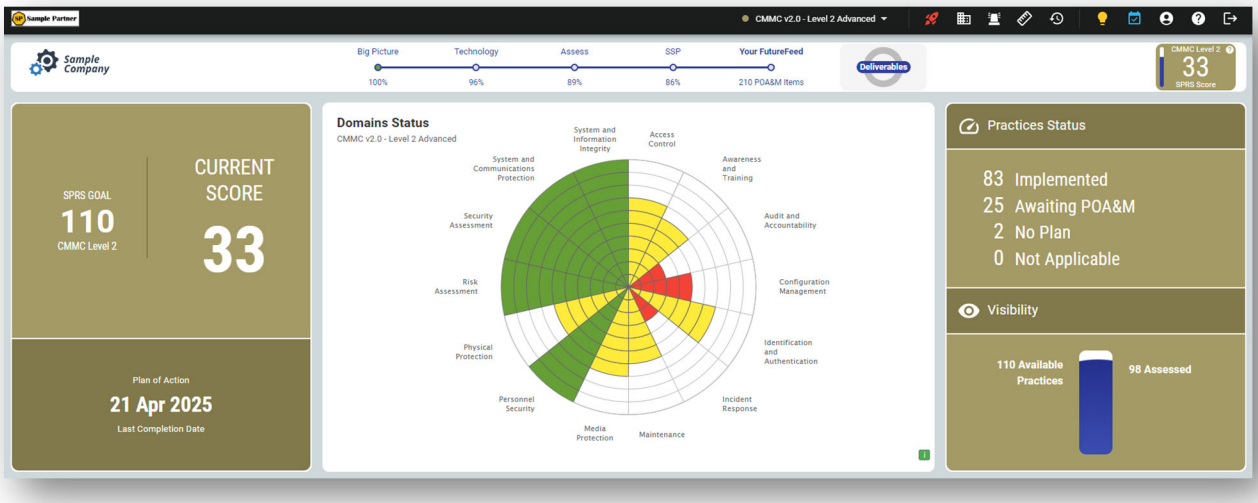
Change is hard for any organization. When it comes to the kinds of changes needed to address today's cybersecurity risks, one key problem is that getting from zero to done is overwhelming. Even with the help of free publications like FIPS 199/200 and NIST SP 800-171A, organizations struggle to understand how to design and execute a cybersecurity program that will protect them while still allowing them to successfully serve their clients/constituents.



The Solution: FutureFeed™

That is where FutureFeed comes in. FutureFeed isn't yet another high-tech toy filled with buzz words like "Artificial Intelligence" and "Machine Learning" that is destined to sit silently in the corner. Instead, FutureFeed is a tool that encourages organizations to embrace and adopt cybersecurity as part of their DNA while still allowing them to deliver their core products and services.

FutureFeed empowers organizational leadership with confidence that their cyber program is aligned with their business needs and regulatory requirements. FutureFeed gives the organization's leaders unprecedented visibility into the cyber risks their organization faces, as well as control over their organization's approach to addressing those risks.



FutureFeed Overview

From ensuring that policies and procedures are created and followed to validating that known vulnerabilities are patched in a timely manner, managers use FutureFeed to keep their operations running smoothly and effectively. All without a bunch of technological gobbledygook.

Attain. Maintain. Prove it Anytime.™ That's more than the FutureFeed motto. It sums up FutureFeed's capabilities and illustrates how FutureFeed excels beyond its competition.

Unlike most other tools, FutureFeed wasn't built by techies for techies. Instead, FutureFeed was developed for an organization's leadership by a team that includes highly experienced senior corporate leaders, entrepreneurs, software developers, IT and cybersecurity assessors, service providers, lawyers, and educators. They came together to build FutureFeed, a service that makes cybersecurity accessible to the C-Suite by ensuring the organization's program aligns with industry standards.

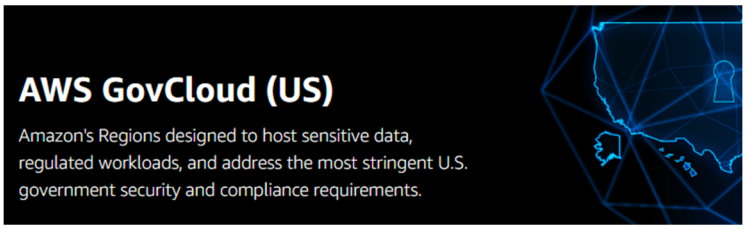
The FutureFeed platform walks clients through the process of documenting their current IT and cybersecurity programs, identifying gaps in their current efforts as compared to industry standards, creating and executing plans to remediate those gaps, and, most importantly, continually monitoring their programs once the gaps are closed to ensure they stay secure.

Security Without Governance is not Secure

While other so-called compliance tools focus exclusively on a companies' short-term needs of preparing for an assessment, the FutureFeed platform delivers tools for the long-term, helping organizations develop and manage their cyber compliance programs. From creating and reviewing policies and procedures; to conducting and cataloging the types of information processed, stored, and transmitted by the organization's systems; to dynamically building and maintaining an organization's system security plan ("SSP"); to tracking new ideas for improving the organization's systems, the FutureFeed platform's robust features enable organizations to build and manage strong and demonstrably secure systems.

Security at its Core

The FutureFeed platform was designed with security in its DNA. All data and compute resources reside in the AWS Gov Cloud, a FedRAMP High authorized environment. The FedRAMP High authorization means the environment is trusted by the US government to store, process, and transmit highly sensitive information, including Controlled Unclassified Information. Leveraging the AWS Gov Cloud ensures FutureFeed has a strong, resilient, and secure core.



The AWS Gov Cloud core isn't the only secure part of FutureFeed. The environment also includes extensive monitoring and alerting capabilities that keep a watchful eye for malicious activity. The FutureFeed development team also leverages a robust suite of static and dynamic testing to ensure the platform is free of known and common coding vulnerabilities. We even employ a team of penetration testers who regularly probe the FutureFeed platform for potential weaknesses.

Relied on by Service Providers

FutureFeed's numerous capabilities, combined with a comprehensive approach to security, mean FutureFeed's appeal isn't limited to individual organizations. The FutureFeed platform has quickly gained a reputation as the go-to solution for managed service providers and consultants, too. These organizations recognize that they must be ready, at any time, to demonstrate that the cybersecurity programs they build for their clients are meeting or exceeding industry standards. Otherwise, when a breach occurs, the client will point the finger at, and seek compensation from, the service provider. FutureFeed's easy-to-understand dashboards and dynamic report generator allow service providers and clients alike to see the work that is being done and to prove compliance at any time.

> *"I used to try to manage the compliance through spreadsheets and that was really painful and lacked clarity. After reviewing many software tools, I can honestly say you'd have to rip FutureFeed out of my cold dead hands. It has been an invaluable tool to assuring we are on the right track for our client's compliance."*
> Leia Shilobod, CEO, InTech IT

Ready for Assessments

Not only does FutureFeed give organizations and service providers a powerful set of tools for managing their compliance programs, but it also makes it easy for the organizations to demonstrate their

compliance to independent assessors, auditors, regulators, and other interested parties. All of this, at the push of a button. Anytime. When the CMMC program kicks into high gear in early to mid-2023, FutureFeed's clients will be well positioned to continue doing business with DoD and the rest of the federal government.

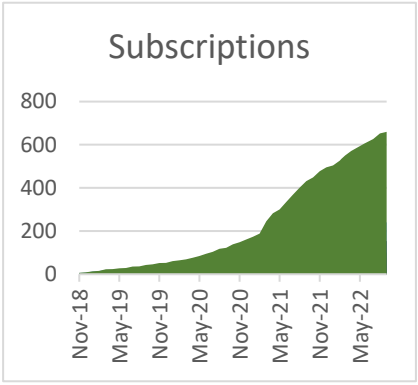
Cost-Effective Subscription Model

You're probably thinking "I have a lot of people who would need access to FutureFeed. I bet this is expensive." Unlike our competitors, FutureFeed isn't priced on a per-seat or other metered usage model. Instead, you pay a single subscription fee for each managed environment, and you can add as many users and documents, and as much other information, to FutureFeed as you'd like without any additional fees.

Our clients routinely tell us that our fee model results in significant cost savings over our competitors. We even offer discounts for small and medium businesses (those with fewer than 200 employees) and even bigger discounts for innovative, start-up size companies (those with 20 or fewer employees). This means your organization has one less speed bump on its path to a secure future.

Trusted by Many

As a result of the powerful, comprehensive, and cost-effective set of features baked into FutureFeed, the platform has seen wide-spread adoption across, and even beyond, the Defense Supply Chain. In fact, in the span of only a few short years since its release, hundreds of companies of all different sizes and across a wide range of industries have come to rely on FutureFeed to help them implement and manage their cybersecurity programs. FutureFeed's customers have even been audited by the Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC") and passed their audits with relative ease thanks to FutureFeed's unique capabilities.



Furthermore, nearly a hundred service providers are standardizing their cybersecurity offerings around FutureFeed. The result is an ever-increasing number of companies for which FutureFeed is the core to their cybersecurity.

Choosing a Governance Platform

When your organization is ready to stop throwing technological Band-Aids on its cybersecurity program and start implementing a well-designed and governed program, don't just choose any product. Choose a platform designed with security in mind from the ground up. Choose a platform trusted by hundreds of government contractors and nearly a hundred service providers as their platform of choice. Choose a platform that helps you not only attain compliance, but also maintain it and prove it anytime.

Choose FutureFeed.