DSD LABORATORIES

75 Union Ave 978-443-9700
Sudbury, MA 01776 800-432-8484
www.dsdlabs.com Fax: 978-443-6033

Cybersecurity

A DSD Core Competency

Move from DIACAP to RMF without expensive re-work and costly delays

CAGE CODE: 0ABU8 DUNS: 175362755

DSD Talent Space

More than ever before, government and industry are reliant upon increasingly complex technology to operate and maintain business processes while also achieving strategic objectives. For example, the explosive growth of "smart" devices and the cloud, while presenting highly attractive cost savings and productivity gains, also introduces potential vulnerabilities and increased risk. Well-executed cybersecurity can minimize these risks significantly; DSD is on the forefront of creating and applying advanced cybersecurity engineering to combat those threats.

DSD's targeted approach to cybersecurity overcomes shortfalls in traditional and agile development methodologies that typically leave security to be addressed too late in the development cycle which drives costly re-work, schedule slips and risks producing capabilities without the proper safeguards of mission data. As depicted in Figure 1, DSD integrates cybersecurity into software development models to provide a holistic model that designs for cybersecurity and proactively reduces operational risks. Through this integrated, innovative, and proven methodology, DSD:

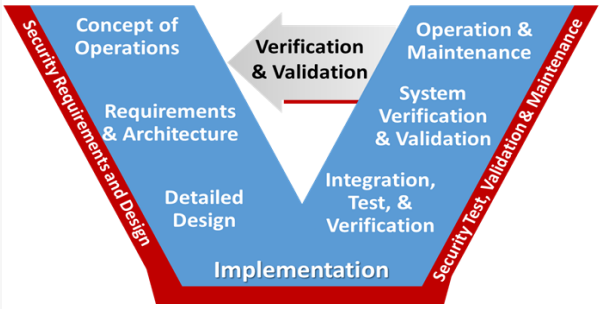

Fig. 1 — V-Model Integrates Software & Security Engineering

- Captures the protective needs of an organization through the detection and evaluation of threats, vulnerabilities and potential impacts to operations
- Analyzes risk trade offs through the assessment of costs and benefits of protective measures
- Designs, builds, tests and maintains protective measures to address vulnerabilities and threats
- Develops ongoing security risk management processes to provide persistent risk management
- Utilizes DSD experience working one-on-one with all levels of the approval process, from senior leaders, to program managers, to programmers and developers

DSD's multidisciplinary security engineers have extensive cybersecurity backgrounds making them well-equipped to perform a wide range of cybersecurity engineering tasks such as business process threat and risk analysis, requirements elicitation, security architecture, threat and vulnerability assessments, computer and communication security, networking, security technology assessments, development, test and evaluation, and penetration testing.

DSD pioneered many of the DoD and AF requested Risk Management Framework (RMF) path-

"DSD came prepared with the experience and current standards that allowed them to quickly, easily and correctly complete the 1,326 individual tests. As a result of that quality, FS was able to complete their Authority to Operate in record time" — Forest Service (FS) CPAR

"The quality of work being done is superb and often the personnel keep in mind the significance of their actions supporting the warfighter" — AFRL CFRDS CPAR

"...phenomenal eMASS experience...efforts helped catapult AFSOC learning curve to instruct/guide the Special Operations Force (SOF) community" — AFSOC/A6 PM

DSD LABORATORIES

"The job is not finished until the customer is satisfied"

DSD Talent Space (cont'd)

finders used to benchmark and test the plans to move from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the National Institute of Standards and Technology (NIST) based RMF – essentially building the RMF program from the ground up. Additionally, DSD has extensive knowledge and experience performing RMF activities for hundreds of federal systems in other agencies including US Coast Guard, USDA, Department of Interior, Veterans Affairs, and Department of Treasury. With DSD's approach and expertise, our personnel provide:

- Tools, techniques, training, and procedures to identify, analyze and quantify vulnerabilities
- Risk based decision models tailored to an organization's risk tolerance that drive the smart application of security resources
- Risk scorecards that communicate risk levels for each security objective

Sound security engineering recognizes that the security features one organization requires may not adequately secure another organization; DSD's tailored approach enables organizations to focus and prioritize valuable security activities, and to:

- Reduce operational vulnerabilities through business reengineering to your cyber workforce
- Avoid costly re-work and schedule delays due to last minute security findings
- Develop resilient, penetration-resistant, and trustworthy systems

This rich comprehensive suite of offerings – from tailored methodologies to practical, reusable tools and templates – is why DSD has 87% repeat customers.

CERTIFIED NWBOC WOMAN OWNED BUSINESS

DIFFERENTIATORS

- CISSP
- ISSEP
- Security +
- CRISC
- FITSP-A
- CSSLP
- OSCP
- CAP
- MCSE +S
- MCSA +S

Past Performance

	HQ AF/A4 Integration, Logistics Management and Mission Support # GS-10F-0319K NAICS / PSC: 541611 / R408 **Contact**: Mr. Jeff Hotmar jhotmar@dsdlabs.com	DSD provided a full suite of management consulting and Information Technology (IT) services to include cybersecurity engineering, Risk Management Framework transition planning, collaborating with NIST and DoD cybersecurity experts and assessing critical systems to the AF logistics operations. **Leader in RMF transition** DSD is the first and only team to pilot the shift to RMF for the entire AF, resulting in the first risk based Assessment and Authorization (A&A) program in the DoD, and providing a model for A4, the AF, and DoD. **Assessment Expertise** Evaluated and recommended security improvements and coordinated approvals for 20 major A4 systems, preventing shut-down directives which would severely impact operations and deny access to thousands of AF users. **Engineering Expertise** Worked side by side with systems engineering to identify protective needs, develop technical designs, implement and integrate cybersecurity into a mission critical logistics system.
	AFLCMC/HNIZ Cybersecurity Assurance Support #FA8771-12-D-1005-0002 **Contact**: Mr. Jeff Hotmar jhotmar@dsdlabs.com	DSD assessed hundreds of AF systems under DIACAP utilizing a highly qualified staff with extensive experience in security analysis, security engineering, and certification and accreditation (C&A). DSD provided expertise in the ongoing transition to the Risk Management Framework (RMF), applying extensive experience performing over 700 RMF assessments .
USDA	Security Services for HRSS # AG3142B070008 NAICS / PSC: 541511 / D310 **Contact**: Mr. Jeff Hotmar jhotmar@dsdlabs.com	DSD provided the full range of Information Assurance/Cybersecurity support services, including IT C&A, independent verification and validation, systems integration, and network engineering; this enabled the accurate identification and verification of 1326 different security controls. Throughout this effort, DSD maintained exceptional quality in NIST 800-53 testing and documentation.