IntelliDyne

EXPERIENCE ABOVE & BEYOND

WHITE PAPER:

# STRATEGIC IMPACT PILLARS FOR OPTIMIZING INFORMATION SECURITY IN GOVERNMENT

IntelliDyne, LLC

MARCH 2012

# STRATEGIC IMPACT PILLARS FOR OPTIMIZING INFORMATION SECURITY IN GOVERNMENT

## Executive Summary

*The rapid expansion and reliance on computing systems, databases, remote access, Internet usage, and processing power has increased the complexity of Information Technology (IT) systems and infrastructure. This increased scope and complexity has also increased the potential for outside attacks and security breaches within the realm of cyberspace. According to an Information Week survey, the No. 1 priority among federal IT professionals is security, with 69% of survey respondents viewing it as extremely important. That reflects the Office of Management and Budget's (OMB) emphasis on "well-designed, well-managed continuous monitoring and standardized risk assessment processes."*[1]

*Information Assurance (IA) and Cyber Security (CS) ensure that data and systems are adequately protected. Implementing an IA & CS strategy involves determining the protection needed; implementing the needed protective measures; assessing the adequacy of the protection; and tracking, managing, and repeating the process to determine how well the data and system remain protected.*

*However, implementing IA & CS policies is much like visiting the dentist: people really don't like going – but, for their own good they go, and typically, it is not cheap. This paper outlines the four strategic pillars that you need to include in your IA &CS policies to minimize the pain points and maintain robust security of your IT systems.*

[1] InformationWeek 2011 Federal Government IT Priorities Survey

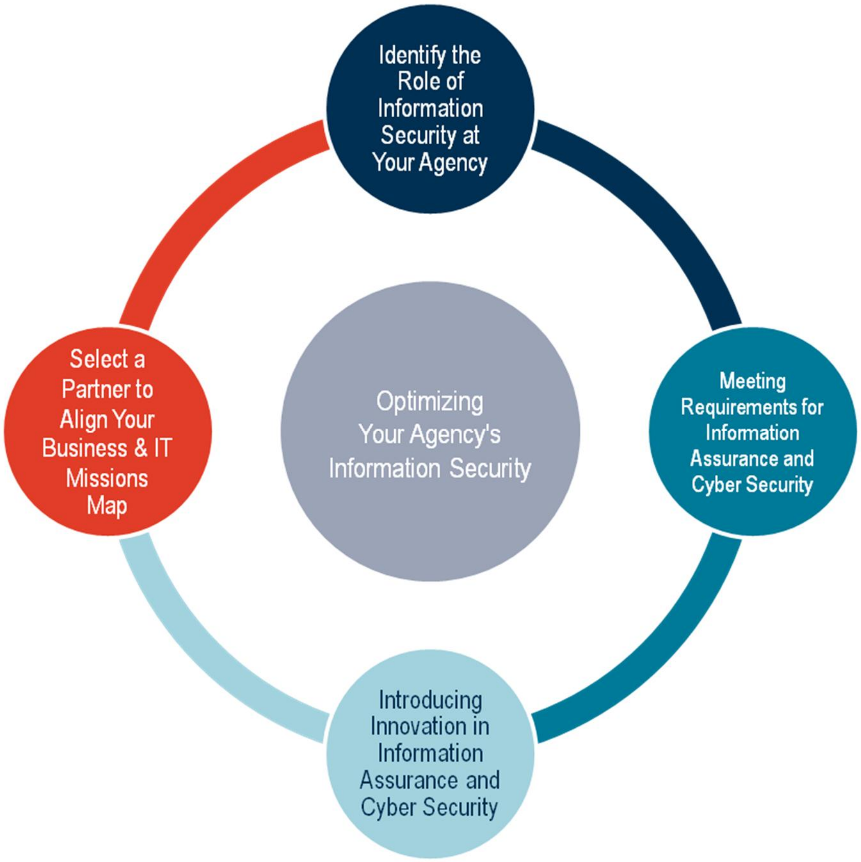

Identify the Role of Information Security at Your Agency
Meeting Requirements for Information Assurance and Cyber Security
Introducing Innovation in Information Assurance and Cyber Security
Select a Partner to Align Your Business & IT Missions Map
Optimizing Your Agency's Information Security

**Figure 1: IntelliDyne's Strategic Impact Pillars for Optimizing Your Government Information Security**

## STRATEGIC PILLAR 1: IDENTIFY THE ROLE OF INFORMATION SECURITY AT YOUR AGENCY TO MEET YOUR BUSINESS MISSION

No matter what agency you're involved with, your systems include complex computer networks, a large number of internal and external users, and vast amounts of sensitive data. To keep your networks secure and your data private, it is vital that an information security plan be put in place.

In technical jargon, the government is becoming more and more focused on ***Compliance and Risk Management***. The truth is there are people seeking access to agency data for malicious purposes. There were 41,776 reported cyber incidents of malicious intent in the federal network in 2010 – this out of a total 107,439 reported to the United States Computer Emergency Readiness Team (US-CERT).[2] In 2010, the Federal Government reported 56,579 phishing attacks, or 52.7% of the total number of incidents. In 2009, it reported 70,132 phishing attacks, or 64.5% of that year's total. The privacy and security of your data

[2] http://www.informationweek.com/news/government/security/229400156

demands that you have a plan in place to thwart these kinds of attacks as attack types evolve, and new attack types are developed.

Another important factor to keep in mind: IA & CS compliance is not merely a technology issue. It is also a governance issue, and all members of executive management, not just the CIO, need to be involved in policy development and implementation so that compliance is maintained and risk management is employed. As stated in the White House's Cyberspace Policy Review, "this approach requires clarifying the cyber security-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions."[3]

## STRATEGIC PILLAR 2: MEETING REQUIREMENTS FOR INFORMATION ASSURANCE AND CYBER SECURITY

Creating a plan to implement IA &CS protocols must be an essential part of your agency's mission. However, it is not necessary to reinvent the wheel when it comes to developing a regulatory strategy. There are many legislative acts that prescribe general IA &CS regulations, such as:

- Sarbanes Oxley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

For example, OMB interpretation requires government entities use NIST guidelines for FISMA requirements. OMB has most recently (2011) given DHS the lead role for the deployment and reporting of Information Assurance activities. For the Department of Defense (DoD), the two critical directives are 8500.1, Information Assurance, and DoD Instruction 8510.01, the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP.) General acquisition regulations such as DoD 5000.1 define the need for IA at a higher level than that indicated by FISMA. Chapter Three of the Information Assurance Technology Analysis Center (IATAC) report "Measuring Cyber Security and Information Assurance" provides significant resources on specific regulations dealing with IA &CS.[4]

Based on the specific data and systems that your agency works with, it is absolutely essential that the relevant regulations are understood and complied with. In addition to varying regulations, the metrics that different organizations use may also vary significantly. The table below, also from the IATAC report, compares the IA metrics used by DoD, the Air Force, and NASA JPL to illustrate this point.[5]

[3] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[4] Bartol, et. al., Measuring Cyber Security and Information Assurance: A State of the Art Report May 2009.
[5] Bartol, et. al., Measuring Cyber Security and Information Assurance: A State of the Art Report May 2009.

| | DoD | Air Force | NASA JPL |
|---|---|---|---|
| **Motivations** | Return on investment, mission readiness (surrogate for effectiveness) | Return on investment, mission accomplishment | Process improvement, implicit return on investment |
| **Primary Objectives** | Determine how to measure strategic objectives, re-use existing data | Determine how to measure strategic objectives, re-use existing data | Improve control over process |
| **Challenges** | Disparity between numerous data sources, too much time spent “cleaning” data, not enough personnel doing analysis, difficult to use massive amount of data collected | Problems managing issues discovered, risks accepted at lower levels make risk unmanageable from enterprise perspective, difficult to use massive amount of data collected | Management intervention still required to enforce policy |
| **Process Complexity** | Extremely high | High | Medium to Low |
| **Drivers** | FISMA, congress, other budget and effectiveness questions | FISMA, congress, DoD questions, improvement of IA posture | Process improvement, responsibility to sponsors |
| **Orientation** | Bottom-up, attempting to tie toward high objectives | Bottom-up | Top-down |
| **Strengths and Keys to Program** | Long history – co-developed most standards, many data sources | Air Force has increasing role in cyberspace so program should be put at forefront, many data sources | Track record of success, credibility with leadership as well as other agencies like NIST, asset control |
| **Approach to Automation** | Desired but not there yet | Desired but not there yet | In place and successful |
| **Time to Market from Policy to Implementation** | Very slow | Very slow | Moderate |
| **Type of Metrics Collected** | Heavily technical but also containing operational and management metrics | Heavily technical but also containing operational and management metrics | Mix of technical, operational and management-related |
| **Style of Data for Majority of Metrics** | Nominal, Boolean checklist-oriented questions | Nominal, Boolean checklist-oriented questions | Ratio |
| **Program Successes Perceived by Organization** | Not yet successful | Not yet successful | Successful and improving |

**Figure 2: IA metrics used by DoD, the Air Force, and NASA JPL**

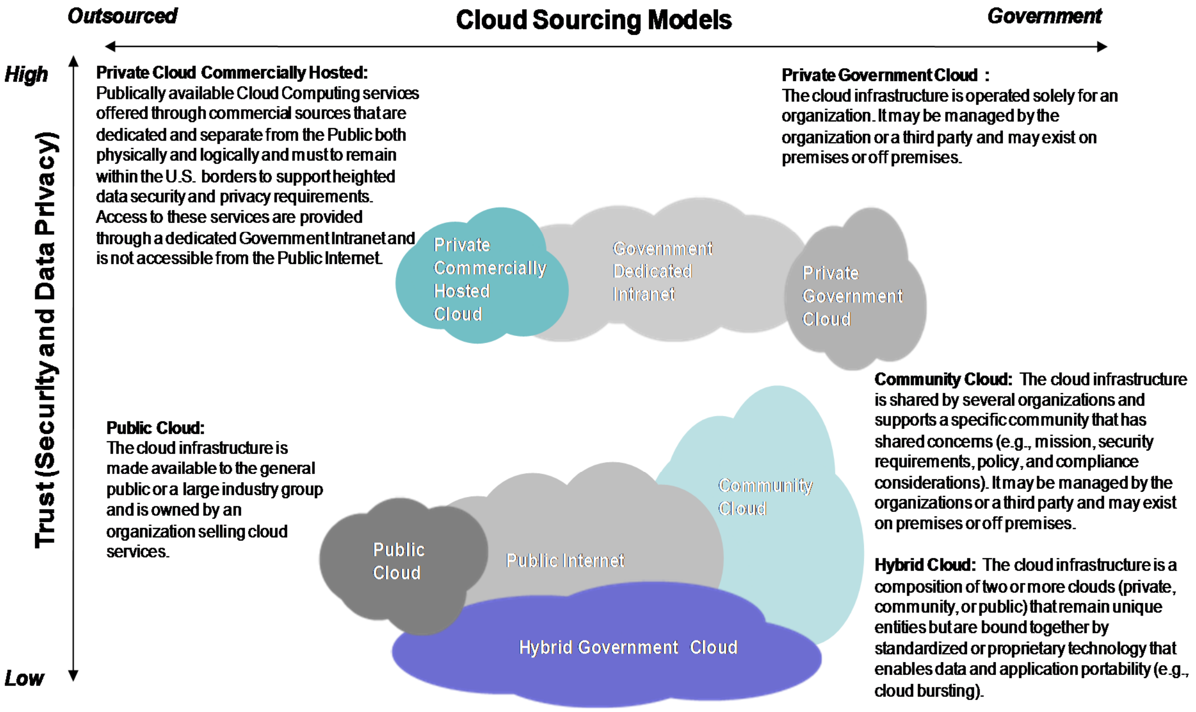
## STRATEGIC PILLAR 3: INTRODUCING INNOVATION IN INFORMATION ASSURANCE AND CYBER SECURITY

In many cases, the regulations are clear, but the processes for implementation and governance of IA & CS are not. The world of cyber security is evolving rapidly and in every aspect – from government regulations changing to cyber-attacks becoming more and more prevalent and difficult to decipher. As a result of the speed with which the industry is changing, keeping pace is difficult and essential and to do so requires constant innovation. It may seem obvious that every task has a written process and procedure, but often the documentation does not exist. The National Initiative for Cyber-security Education (NICE) and organizations like SANS have broken down IA & CS into teaching segments, but not into basic task areas. FISMA and ISO 17799 also provide useful inputs into governance framework. The former includes management templates for federal agencies. ISO 17799 includes general IS implementation guidelines that can be tailored to the needs of each entity.

IA & CS are no longer just technology considerations – it must involve every aspect of an organization. Every role within an organization must be empowered to implement security decisions, and contribute to the security rules creation. In the past, security strategy, implementation and governance has been viewed as the responsibility of IT personnel alone. To obtain effective information security, this attitude cannot continue; It is imperative to move beyond the traditional approach and make IA & CS more meaningful and functional on the day-to-day business level. Technology must be used more effectively and the appropriate people in departments and organizations across the enterprise should continually be given the tools to do so.

This enterprise-wide approach is important; it paves the way for a simplified means to security and innovative ways to implement technology. It enables the government and the agencies within it to describe the level of security it wants, to view security as concentric circles that can be drawn around the focal point of what needs to be secured, and to not redefine the meaning of borders and perimeters. It allows the use of a modular approach and the ability to change one aspect without changing everything else.

The Federal Government has been developing top-level guidelines for dealing with IA &CS in a world where more and more data is being transitioned to cloud computing and mobile access. The figure below, developed by the Federal CIO Council, illustrates the balance of trust needed when developing cloud sourcing models.[6]



**Private Cloud Commercially Hosted:** Publically available Cloud Computing services offered through commercial sources that are dedicated and separate from the Public both physically and logically and must to remain within the U.S. borders to support heighted data security and privacy requirements. Access to these services are provided through a dedicated Government Intranet and is not accessible from the Public Internet.

**Private Government Cloud :** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises.

**Public Cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

**Community Cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

**Hybrid Cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting).

Figure 3: Cloud Sourcing Models

[6] State of Public Sector Cloud Computing, CIO Council, May, 2010.

However, the challenge with a modular approach is that traditionally, many areas of IA &CS are controlled by different parties within an agency. A top-level governance plan will provide an umbrella of management over each of the individual parties involved in tasks such as information systems security engineering, configuration control management, departmental accreditation, and personnel training.

The IATAC created a practical measurement framework for IA &CS in 2009, presented below, that is still relevant today.

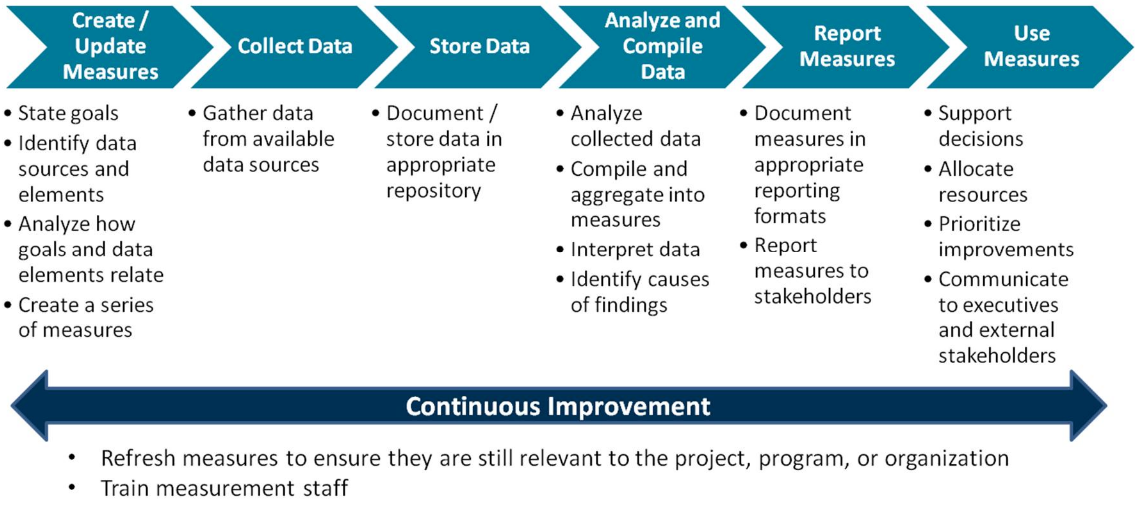

Create / Update Measures
Collect Data
Store Data
Analyze and Compile Data
Report Measures
Use Measures
• State goals
• Identify data sources and elements
• Analyze how goals and data elements relate
• Create a series of measures
• Gather data from available data sources
• Document / store data in appropriate repository
• Analyze collected data
• Compile and aggregate into measures
• Interpret data
• Identify causes of findings
• Document measures in appropriate reporting formats
• Report measures to stakeholders
• Support decisions
• Allocate resources
• Prioritize improvements
• Communicate to executives and external stakeholders
Continuous Improvement
• Refresh measures to ensure they are still relevant to the project, program, or organization
• Train measurement staff

**Figure 4: Information Assurance Technology Analysis Center (IATAC) framework**

For years the information assurance world has pointed to the folly of looking for a single solution – "there is no 'silver bullet'" has been a standard saying – and rightfully so. But while there may be no single silver bullet, indeed relying on a single bullet would create a dependency that would in and of itself be a weakness. There is, however, a six-shooter or more of "silver bullet" technologies that can be pulled together to create any secure environment that is needed based on the risk assessment.

## STRATEGIC PILLAR 4: SELECT A TRUSTED PARTNER THAT UNDERSTANDS YOUR MISSION, NOT JUST THE TECHNOLOGY

To make a difference, it must be understood that many people are focused on titles of the type of work (i.e. Certification and Accreditation or Computer Network Defense), but despite the consistent reference, no two tasks under those titles are the same. Set your focus on ensuring that you and your agency know what specifically needs to be done. Every area of IA & CS has a core group of tasks associated with it – for example "Certification and Accreditation support" does not have a single meaning or set of tasks – but may be any number of tasks that are brought together to meet the client's needs. There will be a core set of tasks that will typically be done and others that may or may not be required.

All things considered, IA &CS management could easily become a commoditized service evaluation once the initial business requirement(s) have been completed. But here, perhaps, lies the largest potential risk in effectively reaching your goals and meeting your mission: whom should you trust with your IA &CS requirements?

This is where using a trusted partner to develop and implement your IA & CS policies can ensure a streamlined deployment process. There is a significant difference between solution providers who are simply technology-centered and those who understand the business and governance impacts that an IA & CS strategy can entail. Ensure that your choice for solution provider is asking not only the important technical questions but also the critical governance questions.

## About IntelliDyne, LLC

IntelliDyne is a consulting firm that enables better business performance through innovative technology solutions. We manage public sector programs that deliver higher operational efficiency and measurable value to clients. We advise, develop, and execute effective solutions in Cyber Security, Cloud Computing, Application Development, Mobile Computing, Business Process Management, Data Center Consolidation, Enterprise Collaboration and Enterprise Infrastructure Management.

For more information, visit our web site at www.intellidyne-llc.com or contact us at IA-Cyber@intellidyne-llc.com.