

# Security for Government Agencies

Improve Secure information Sharing and Regulatory compliance for Public Services

## Many Stakeholders, Incompatible IT landscapes

Government agencies today manage a complex, large, interconnected IT landscape that have evolved over decades and are hard to disentangle, manage and update. This is a major challenge. Many efforts are currently undertaken to design and build a common architectural standard for a joint-up, agile business-driven technology architecture. However, the complexities are often enormous: Service based architectures (e.g. Service Oriented Architectures, SOAs), process-centric architectures (BPM), as well as data-centric architectures (e.g. DDS) are all being deployed alongside more traditional application integration platforms (e.g. JavaEE, JMS, CORBA/CCM).

## Rapid Regulatory Compliance and Policy Implementation

A major task of government agencies today is to implement complex, ever-changing, ever-increasing security-related laws, regulations, and internal policies across a large number of systems and organizations or sub-organizations. Many of these include provisions that need to govern and audit information flows, data usage, data sharing etc. Strong security needs to be demonstratively implemented across a highly complex, interconnected IT landscape that comprises many stakeholders, many legacy systems, and frequent system changes. Cost-effective, automated, agile, low-risk security policy management is a critical aspect in the overall picture.

## Security Compliance Is Business-Led

The business function should drive the security compliance requirements as part of their overall business risk management, and the IT landscape should reflect these requirements. However, many organizations today resort to a part-solution by producing and signing off compliance and best practice documentation, while there is little traceable correspondence to the actual IT landscape and operations. Moreover, incident monitoring is typically done rather ineffectively, which results in incorrect or late responses to security incidents.

## Security Policy Management

Using ObjectSecurity OpenPMF, government agencies can state their security compliance requirements closer to the regulations. OpenPMF turns those requirements into concrete enforcement across the IT landscape at run-time, and monitors compliance at all times. Regardless whether the aim is IT cost optimization or improved service, ObjectSecurity OpenPMF can help you manage security better for new deployments, as well as for redevelopments and legacy application integration.



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a "model-driven security" approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

## Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

[www.objectsecurity.com](http://www.objectsecurity.com)