# DMTF Virtualization Protection Profile
# Incubator Charter

## Dated 07/26/2010

**Ver : 0.3**

The information provided below is subject to change and reflects the current state of the Incubator.

## Management Problem(s) and Environment

In accordance with their respective responsibilities under Public Law 100-235 (Computer Security Act of 1987), the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have agreed to cooperate on the development of security requirements for key technology areas necessary for the protection of Federal information systems and networks, including those comprising the critical infrastructure within the United States.

Virtualization technologies are a key technology and are being used within critical infrustructures within the United States.

NIST and NSA have the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

- To meet the needs of government and industry for cost-effective evaluation of IT products;
- To encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- To ensure that security evaluations of IT products are performed to consistent standards;
- To improve the availability of evaluated IT products.

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, and acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

## Incubator Scope & Charter

This protection profile needs to define the *information flow control, resource isolation, trusted initialization, trusted delivery, trusted recovery domain isolation, identification, authentication* and*audit* capabilities of virtualization technology. The isolation and information flow policies will be defined by the virtualization system's configuration data. A conformant product definition will also include the support technologies and procedures used to accurately generate and securely distribute that configuration data. Specific assurance requirements need to be defined for those support technologies and procedures including:

1. Installation (trusted delivery?)
2. Startup/Shutdown (trusted initialization?, includes sleep and other power state changes)
3. Operational (users and user interfaces—basically, how users interact with the system, probably includes I&A)
4. Trusted administration of platform (remote and local) (especially update, patching, audit mechanisms).
5. Isolation/Architecture (isolation of VMs and VM communications from each other and from the platform's TCB).
6. Programmatic requirements (relating to acquisition, maintenance, assessment of vulnerabilities, generation and distribution of patches, updates)
7. Development/Testing (software development practices, etc.)
8. The output of the Incubator is a Protection Profile targeted to the NIAP (National Information Assurance Partnership) process.

## Business Justification

A virtualization system evaluated against this PP provides a highly robust foundation for system services and applications in mission-critical systems, and a high degree of assurance for the enforcement of related security policies. Such policies include those for the management of classified and other high-valued information, whose confidentiality, integrity or releasability must be protected. For example, VPP separation mechanisms, when integrated within security architecture, are appropriate to support security policies for government, and commercial sectors.

## Expected Incubator Input

- A draft Virtualization Protection Profile from NSA

## Incubator Deliverables

- An incubator updated Virtualization Protection Profile

## Incubator Timeline

The VPP Incubatoris expected to complete the above deliverables within 12 months from approval of the charter by the board.

## Alliance Partnerships

- Trusted Computing Group (TCG)
- Cloud Security Alliance (CSA)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)
- National Information Assurance Partnership (NIAP)

## Reliance/Coordination with other WG Models

- The Systems Virtualization, Partitioning, and Clustering Working Group including all profiles and the OVF specification.
- And others TBD

## Interim Chairs

Winston Bumpus - VMware Inc. - wbumpus@vmware.com

## Supporting Companies

The following leadership or board companies are interested in the formation of a DMTF Incubator to address the problems identified in this document.

- **AMD** – Valerie Kane valerie.kane@amd.com
- **Citrix** – Shishir Pardikar shishir.pardikar@citrix.com
- **IBM** - Dimitrios Pendarakis dimitris@us.ibm.com
- **Intel** – Billy Cox billy.cox@intel.com
- **Microsoft –** Josh Cohen joshco@microsoft.com
- **Oracle –** Mark Carlson mark.carlson@oracle.com
- **VMware, Inc**. – Winston Bumpus wbumpus@vmware.com

## Participation Requirements

Addition of new leadership board members requires a SUPER MAJORITY (75%) of the Review Board.

## Leadership Board Voting Policy

Review Board Voting will be a SUPER MAJORITY (75%) of the Review Board.

## Change log

| | | | |
|---|---|---|---|
| 0.1 | 07/26/10 | Winston | Initial Draft |
| 0.2 | 07/26/10 | Winston | Added Inputs, Deliverables, and Timeline |
| 0.3 | 08/03/10 | Winston | Added Participation Requirements and Leadership Board Voting Policy |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |