

MULTI LEVEL SECURITY, PALANTIR & ICD 501



Asher Sinensky, PhD
Forward Deployed Engineer

Overview

- What is ICD 501?
- What is Multi-Level Security?
- What's the connection between ICD 501 and Multi-Level Security?
- How is Multi-Level security achieved today?
- A Demonstration of Multi-Level Security

ICD 501

INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 501



J. M. McConnell

Director of National Intelligence

21 JAN 09

Date

DISCOVERY AND DISSEMINATION OR RETRIEVAL OF INFORMATION WITHIN THE INTELLIGENCE COMMUNITY

(EFFECTIVE: 21 JANUARY 2009)

ICD 501, Cont.

- ICD 501 succinctly outlines the **roles, rights** and **responsibilities** of the Intelligence Community (IC) with regards to the ‘Discovery and Dissemination or Retrieval of Information within the Intelligence Community’.
- A review of these policies reveals that many of the outlined responsibilities will require the adoption of new technologies to maximize their effectiveness.

6 Policies Related to Technology in ICD 501

- *Responsibility to Provide*
- *Responsibility to Discover*
- *Responsibility to Request*
- *Privacy Rights and Civil Liberties*
- *User Authorization and Auditing*
- *Responsibilities of IC Leaders*

ICD 501 Compliance

- These policies are all quite difficult to meet in isolation and almost impossible to meet in combination.
- Palantir is the only product that does meet all of these requirements out-of-the-box today
 - (see our white paper)
- But what does this have to do with Multi-Level Security?

What is Multi-Level Security?

Multi-Level Security refers to a security environment in which -
many users with:

multiple and varying access permissions

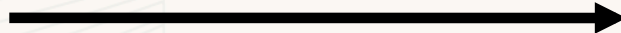
can utilize data with:

multiple and varying access restrictions

ICD 501 means Multi-Level Security

- The first 3 issues = Providing Data Access
 - *Responsibility to Provide (D.2.a)*
 - *Responsibility to Discover (D.3)*
 - *Responsibility to Request (D.4.a)*
- The next 2 issues = Restricting Data Access
 - *Privacy Rights and Civil Liberties (D.6)*
 - *User Authorization and Auditing (E.2.a-b)*

What does this mean in Practice?

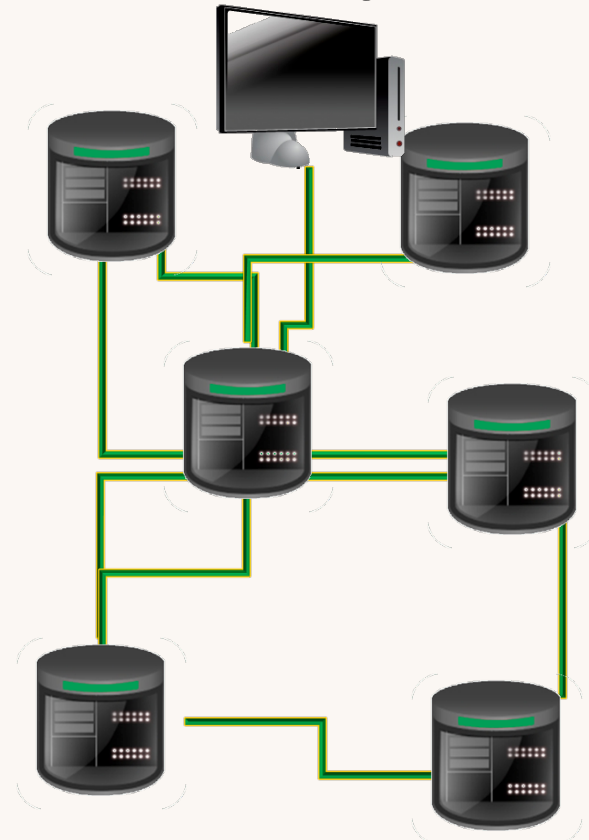
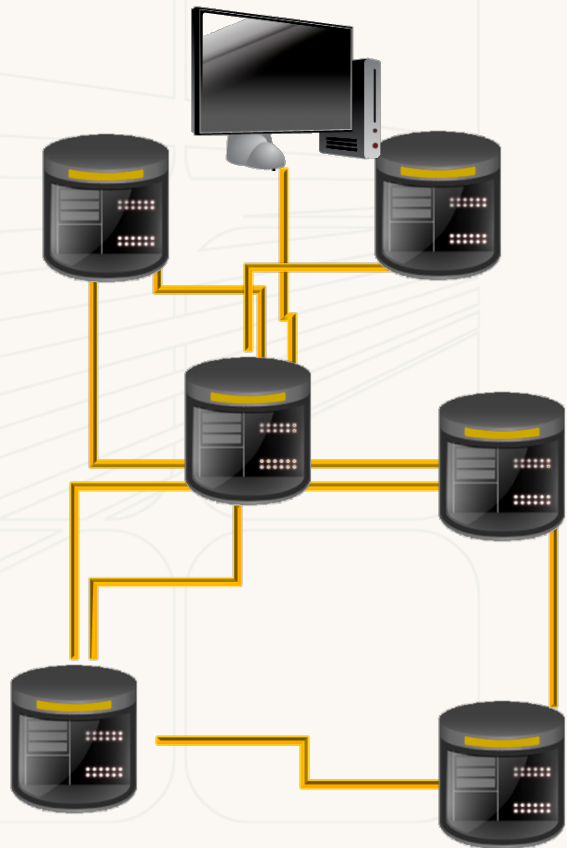


How is this handled today?

- Clearly the current security challenge can be framed in terms of multi-level security
- So how do we deal with this issue today?

...it turns out that in general we don't

Network Level Security



System Level Security

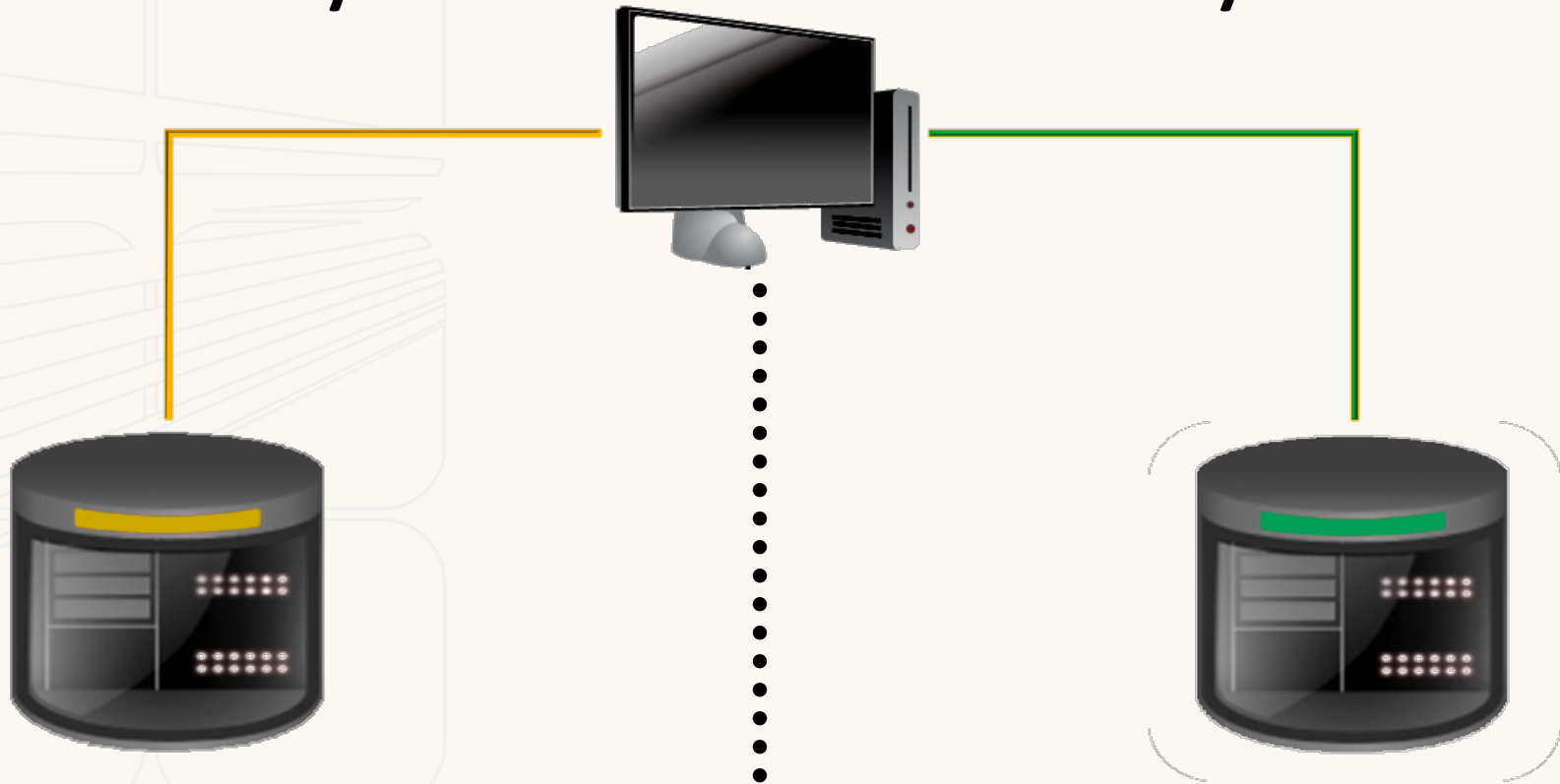
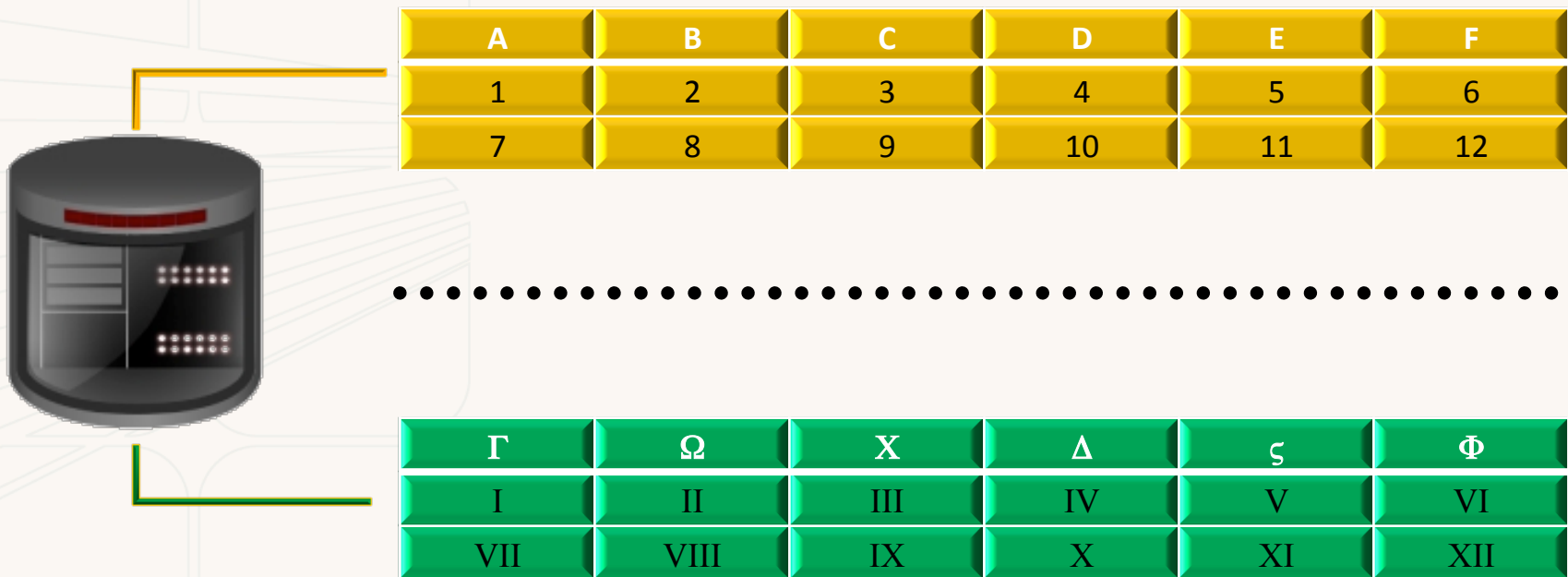


Table Level Security



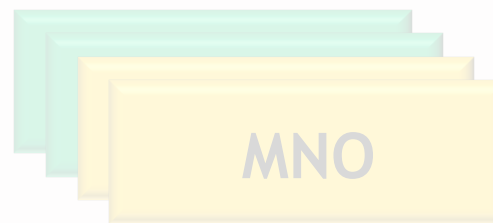
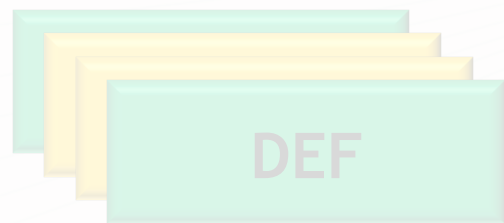
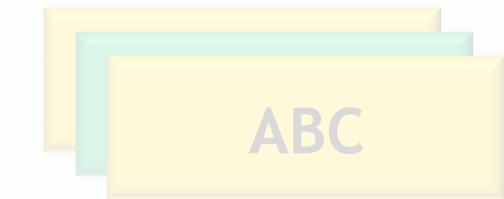
Row Level Security

A	B	C	D	E	F
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

Cell Level Security

A	B	C	D	E	F
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

Sub-Cell Level Security



Each Card may have information about:

- The Value of the Cell
- When the Cell was Created / Modified
- Which User Created / Modified the Cell
- The Access Control on the Specific Card
- The Source from Which the Card was Derived

Access and Permission with Sub-Cell Level Security



Access Control Restricted To:

- Group 1
- Group 2
- Group 3



User Granted Permission To:

- Group 3
- Group 4
- Group 5



The Degree of Access

DEF

Access Control Restricted To:

- Group 1: *Write*
- Group 2: *Read*
- Group 3: *Discovery*

Degrees of Access:

- *Owner*
- *Write*
- *Read*
- *None*
- *Discovery*

Let's Actually take a Look



Administrator –

- Has access to all data



User One – the Unclassified User

- Un-Classified Data
- Program A Data*



User Two – the Classified User

- Un-Classified Data
- Classified Data

And the Beat Goes on

Testimony Of Jeffrey H. Smith¹
Senate Committee on Homeland Security and Governmental Affairs
March 17, 2010

“Shortly before leaving office, Director McConnell issued a directive, Intelligence Community Directive 501... ICD 501 moved the Community very much in the right direction. ***We need to press for complete implementation of that directive.***”

“The stove pipes are still there and we still have much work to break through them.”

Conclusions

- ICD 501 means Multi-Level Security
- Palantir meets the requirements of ICD 501 out-of-the-box today
- *Responsibilities of IC Leaders (G.2.i)*

Questions?

and Thank You