



THE
HUME
CENTER

TED AND KARYN HUME CENTER FOR
NATIONAL SECURITY AND TECHNOLOGY



VirginiaTech
Invent the Future

Ideas for Cybersecurity Leadership by the Commonwealth

T. Charles Clancy, Ph.D.

tcc@vt.edu

<http://www.cyber.vt.edu>

Concepts

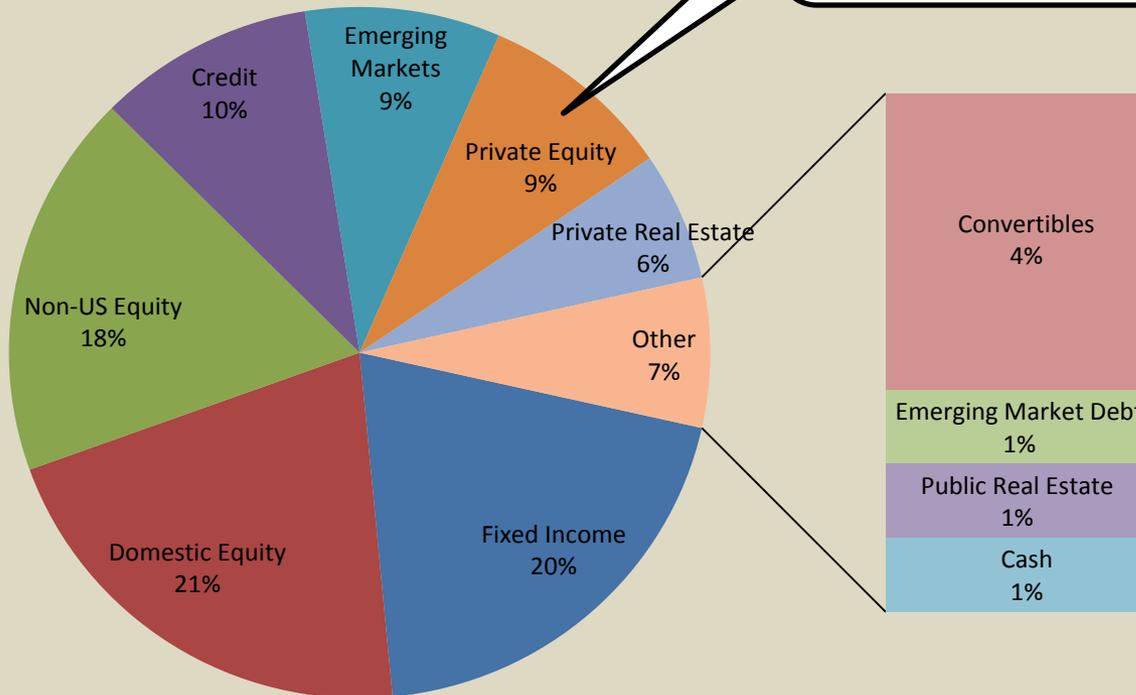
- 1. In-State Private Equity Program** – allocate a portion of the VRS fund to invest in Virginia technology companies working in cybersecurity
- 2. Incentives to Secure Critical Infrastructure** – lead the nation in securing infrastructure against growing cyber threats

In-State VC/PE Program

- Purpose: to attract and retain the best and brightest entrepreneurs to VA and foster future VA job creators
- Concept: commit a portion of the PE allocation within the VRS fund to invest in Virginia technology companies working in cybersecurity
 - VC/PE company must fund 50% in Virginia-based companies
 - Company expenditures should principally be on Virginia-based jobs
- Key Points:
 - **0.67%** of overall VRS fund committed within 3 years
 - Continue management by venture capital and PE firms
 - Communicate broadly; incorporate as part of Virginia's business friendly policies
 - Funds give priority to technology companies working in cybersecurity
 - Synchronize with CIT GAP fund investment priorities

In-State VC/PE Program

VRS Asset Allocation, 2011



Commit ~7% of PE allocation to in-state VC/PE investment

Allocation	Value	%
Total	\$55.00B	100.0
Current PE	\$5.20B	9.3
Proposed In-State PE	\$0.37B	0.7

Commit a portion, roughly \$370M, of the existing PE allocation to program. This is less than 1% of the VRS fund.

In-State VC/PE Program

Example of program success: NY Pension Fund

- Started in 2000
- Committed \$1B to the program since then
- \$615M invested (\$385M still available)
- **>30% Internal Rate of Return**
- 3,000 new employees across 224 companies
- Helped companies raise \$4B additional capital

Incentives to Secure Critical Infrastructure

- Purpose: to lead the nation in securing vulnerable critical infrastructure from cyber attack
 - “over 50% of [industrial] control systems suppliers use default factory passwords” for critical infrastructure
 - Joe Weiss, critical infrastructure security expert*
 - With lack of national legislation and available “low-hanging fruit”, Virginia can demonstrate leadership
- Concept:
 - Funding (either tax credits or grants) to utilities funding critical infrastructure upgrades to support security best practices
 - Commonwealth subsidizes cost for companies to upgrade security to meet newer security standards
 - ... and exceed current requirements

Incentives to Secure Critical Infrastructure

- NIST published SP800-82, “Guide to Industrial Control Systems (ICS) Security” in June 2011
 - “Special Publication” is non-binding, best-practices guide
 - Represents broad range of relatively pedestrian safeguards for critical infrastructure security
- FERC (Federal Energy Regulatory Commission) requires NERC (North American Electric Reliability Corporation) to enforce 8 cybersecurity standards
 - Focus on inventory/reporting, and NIST does not believe they offer sufficient safeguarding
 - FERC does not currently require NIST SP800-82

Incentives to Secure Critical Infrastructure

Current Standards

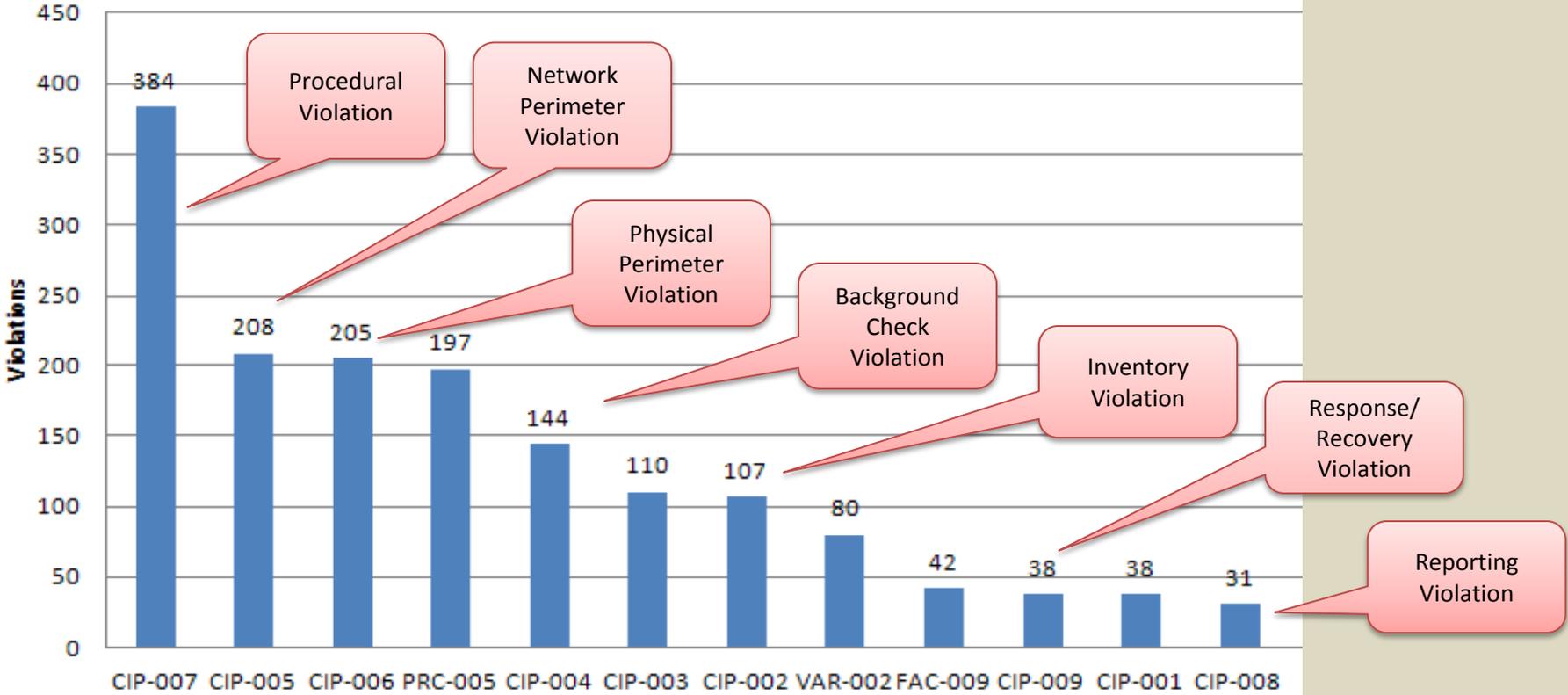
FERC Critical Infrastructure Protection Policies	
CIP-002-4	Identification and documentation of Critical Cyber Assets
CIP-003-4	Development of security policies
CIP-004-4	Background checks for personnel with access
CIP-005-4	Network perimeter and access control
CIP-006-4	Physical perimeter and access control
CIP-007-4	Development of methods/procedures to secure Critical Cyber Assets
CIP-008-4	Incident reporting and response planning
CIP-009-4	Recovery planning and continuity

Emphasis on self-regulation, with operators defining the rules under which they will then be held accountable

Incentives to Secure Critical Infrastructure

Source: NERC.COM

**Top 12 Enforceable Standards Violated
(Active and Closed)
From September 2011 to August 31, 2012**



Conclusions

- These concepts could address material challenges within the Commonwealth, that of:
 - Capital and talent flight to silicon valley start-ups
 - Critical infrastructure egregiously vulnerable to cyber attack
- These ideas are consistent with the Commonwealth platform of leadership in cybersecurity