JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

NIST “RMF” – Engineering, not DIACAP by another Name

NIST Cybersecurity Risk Management Conference

November 8, 2018

Gary Stoneburner
Senior Professional Staff, Johns Hopkins University Applied Physics Laboratory
Gary.Stoneburner@jhuapl.edu

DISCLAIMER: Presentation represents the opinions of the presenter as one of the authors of the NIST guidance with decades of experience with that guidance and its use. The presentation does not represent opinions of Johns Hopkins University Applied Physics Laboratory nor of NIST

Couple of definitions up front:

DIACAP - DoD Information Assurance Certification and Accreditation Process (the 'old' DoD process for cybersecurity)

RMF – Risk Management Framework (a phrase with multiple meanings)

Presentation Purpose

- Speaker's perspective on
  - Current, common state-of-affairs managing controls not risk
  - Engineering focus drove the development of the NIST guidance
  - "Real real" of what controls and baselines actually provide
  - Steps toward actual risk management for mission success

DIACAP-Like (What is it?)

- Process: Pre-defined ‘what to do’
  1. Define high level system characteristics (e.g., unclassified/classified, mission impact)
  2. Based upon these characteristics, apply pre-determined set of security controls

- Rationale: ‘Cybersecurity’ is too hard for the system owner to figure out, so define it for them (that is, in policy)

DIACAP-Like (The problem)

- Problem: Security controls from these DIACAP-like policies are ***typically non-requirements***
  - *DIACAP example:* ECRG-1 "*Tools are available for the review of audit records and for report generation from audit*"
  - A tool, any tool being just 'available' is fully compliant

- Furthermore: Vague and do not always obtain even what was vaguely stated
  - Witness a program rephrase a control, leaving out the "hard part" ("oh, we never do that part")
    - *Control is addressed by requirement document para xxxxx – 'Tick'*
    - *Certifier response – yup, there it is!*

DIACAP-like ‘cybersecurity’ – Reality Check

- Define at best minimal policy compliance, not cybersecurity capability
- Might not even get what the controls vaguely say
- Has no solid mission needs to hang onto when pressured by other requirements anchored in definitive mission needs – security loses
- Those treating policy-driven ‘security’ as a paperwork exercise are right!
  - That is, other than mitigating risk of the authorizing official (AO) saying ‘no’ (making the AO, in effect, the adversary)

DIACAP-like “security” – appeases policy, not provides capability

RMF –NIST Controls by example (what they really are)

AU-4 Audit Storage Capacity The organization:

Allocates audit record storage capacity in accordance with [_____].

AU-5 Response to Audit Processing Failures The information system:

a. Alerts [_____] in the event of an audit processing failure; and

b. Takes the following additional actions: [_____].

- NIST controls are purposefully ***incomplete***
  - Blanks, multiple choice, and
  - NIST explicitly states may need to add/change text to "*fully define the intent*"

RMF – NIST Controls (Reality Check)

- AU-4 and AU-5 are examples of controls in all three NIST baselines – same incomplete control text whether little or catastrophic impact
- With DIACAP-like “requirements” such as “use AU-4, AU-5, … ”, what information is there to tell us how to complete the controls?

  Answer: nothing, nada, zilch

RMF – NIST Control Baselines (What they really are)

- **NOT engineered** levels of security capability even if you were told how to complete the purposefully incomplete NIST controls
- Starting point **alternative to a blank page**
- "***starting point*** *in determining the security controls*" to be *tailored* –
  - scoped ("*eliminate unnecessary*"),
  - compensated ("*alternative*"),
  - supplemented (add controls to "*sufficiently mitigate the risks to organizational operations and assets, individuals, other organizations, and the Nation*") and
  - Completed (blanks, multiple choice, and changes to control text)

RMF – NIST Control Baselines (Reality Check)

- NIST baselines do not define a cybersecurity capability because no one ‘right’ answer:
  - Knowing cyber risk ≠ knowing what must be done (different risk tolerances, different mission/business drivers)
  - Knowing what must be done ≠ knowing how (different controls can achieve same objectives at different “costs”)
- Bottom line: NIST controls and baselines
  - Work well in NIST’s defined process that requires ‘tailoring’
  - Fail miserably when process presumes baseline = a security capability

Brief History of NIST “RMF”

- And then there was congress:

  Federal Information Security Management Act (FISMA) 2002

    NIST “shall …[provide guidance for] minimum information security requirements … no later than 36 months”

Brief Chronological History of the “RMF”

SP 800-30 Risk Management (2002)

Risk through IT, not to IT

SP 800-30 Rev 1 Risk Assess (2012)

Determine risk (part of original 800-30)

SP 800-53 Security Controls (2005)

RM is (RMF) and is part of control selection process

SP 800-37 Rev 1 Applying the RMF (2010)

RMF has its own home

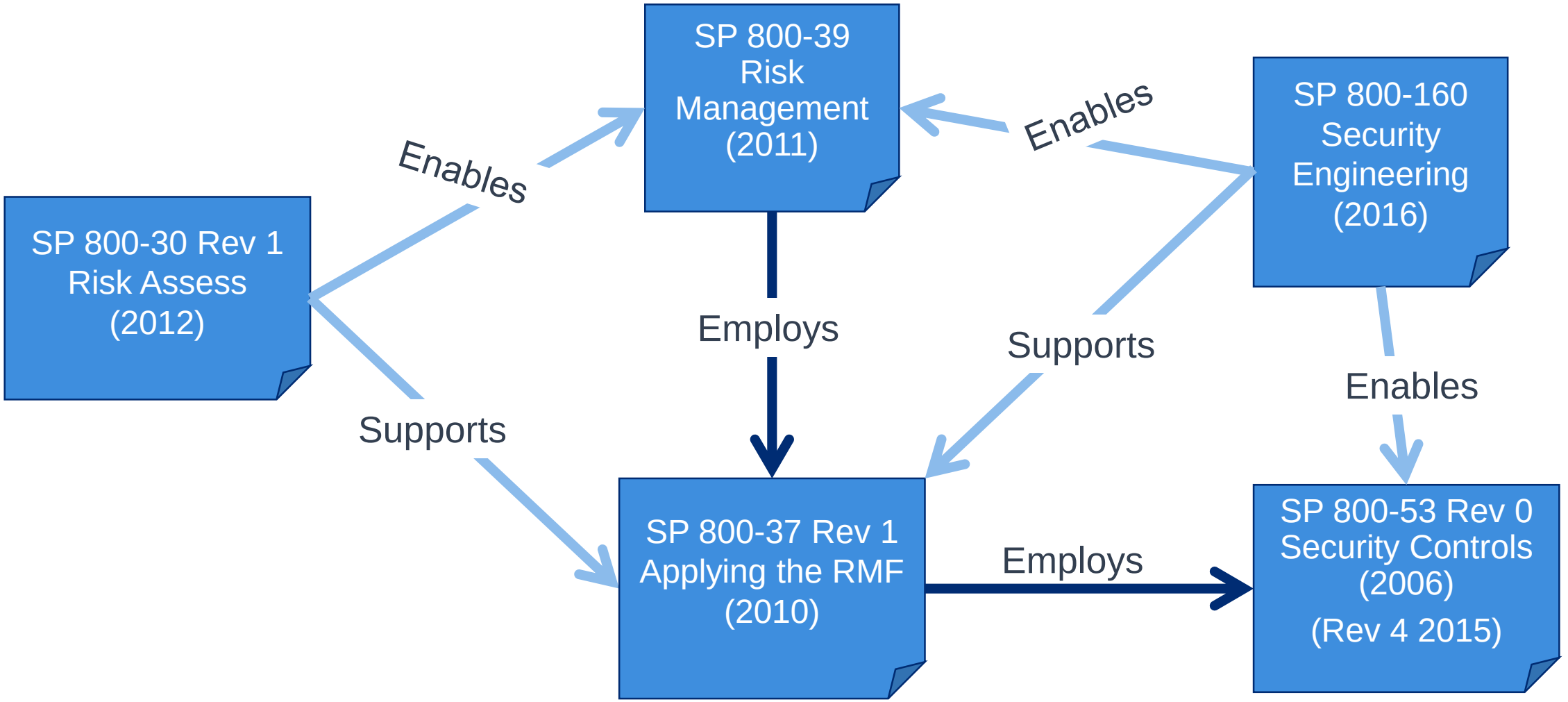
SP 800-39 Risk Management (2011)

RMF now system level of 3 level RM

SP 800-160 Security Engineering (2016)

Engineering for security

“RMF” – Inter-Relationship of NIST Guidance



SP 800-160 Summary - Engineering required

"***Providing satisfactory security controls*** *in a computer system is in itself* ***a system design problem****. A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security. In particular, software safeguards alone are not sufficient.*"

-- The Ware Report , Defense Science Board Task Force on Computer Security, 1970.

"*This publication addresses the* ***engineering-driven actions necessary*** *to develop more defensible and survivable systems …*"

"… *today's systems have dimensions and an inherent complexity that* ***require a disciplined and structured engineering approach*** *to achieve any expectation that the inherent complexity can be effectively managed*"

Quotes from SP 800-160 [emphasis added]

SP 800-160 Summary – Mission-driven Requirements are Essential

Quotes from SP 800-160, Current version, 2018 [emphasis added]

1. "… *security objectives are foundational in that they establish and scope what it means to be* ***adequately*** *secure*" (page 23)
2. *"Protection needs are determined based on the security objectives, life cycle concepts, and* ***stakeholder*** *concerns [and] subsequently transformed into stakeholder security requirements"* (page 23)
3. *"… transforms the stakeholder security requirements into the* ***system*** *requirements that reflect a technical security view of the system."* (page 96)
4. *"… generate system* ***architecture*** *alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a set of consistent views."* (page 101)
   [Quote in document from ISO/IEC/15288-2015]

Security Controls about here

Way-Forward – Engineering Needed – Step 1

Step 1: Reality Check – ***see the real real***

- THE first order, critical need
  - Until reality sets in, substantive change is unlikely
- The real real:
  - Security controls do not state what must be done
  - Control baselines are not definitions of security capability
  - Managing controls is not managing risk

Managing controls – achieving policy and benefiting adversaries

Way-Forward – Engineering Needed – Step 2

Step 2: Answer straight forward (albeit ‘challenging’) questions:

- Does systems engineering ‘own’ cybersecurity like it does other types of requirements?
- Do we have a ‘cybersecurity’ requirements hierarchy that resembles that for other types of requirements?
- Do we have a mission/business reason for each control? Reason for that specific control and not some other, cheaper way or even not at all.

Way-Forward – Engineering Needed – Step 3

Step 3: Answer questions that may be fraught with ‘angst’

- Are those tasked with defining the cybersecurity “requirements” engineers?
- Or have we assigned non-engineers a task only engineers can perform?

Engineer: Expertise and experience to capture complex system requirements without expectation of pre-defined, answers-in-policy

Way-Forward – Engineering Needed – Step 4

Step 4: If you get this far –the rest can come quite naturally because -

- Acknowledging the real real will surface the key question:
  - Is addressing compliance risk good enough?
    - ***If yes –*** then you might be an organization where cyber impact is just a cost of doing business, provided can show ‘due diligence’ – aka policy compliance
    - ***If no*** - then an explicit ‘no’ will drive a felt need for managing risk not just managing controls – aka, engineered solutions not security-by-policy

Final thought

- Measuring ourselves from where we were
  - Is not measuring from where we need to be
- A story …

- A final caution – by managing controls we could be:

  Moving from "*woefully inadequate, to not good enough*"

  - Chris Stoneburner, Red Teamer, JHU/APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Gary.Stoneburner@jhuapl.edu