OPEN Compute Project®

Connect. Collaborate. Accelerate.

ami

Building SBOM for System Firmware

Kelly Bryant, CPO, AMI

Brian Mullen, Senior Manager of Software Security, AMI

May 17, 2022

OPEN SYSTEM FIRMWARE

Connect. Collaborate. Accelerate.

Open Compute Project®

Agenda

- AMI Open-Source Initiatives
- SBOM Overview
- Firmware Supply Chain Challenges
- Strategy
- PoC
- Call-to-Action

AMI IS EMBRACING OPEN SOURCE

Transparency

Reliability

Security

Driving innovation through open-source

- Encourage adoption of industry standard solutions
- Develop with a community-first approach

SBOM Overview

Connect. Collaborate. Accelerate.

Software Bill of Materials (SBOM)

What:

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components -NTIA

Why:

Compliance: Cybersecurity EO of 2021

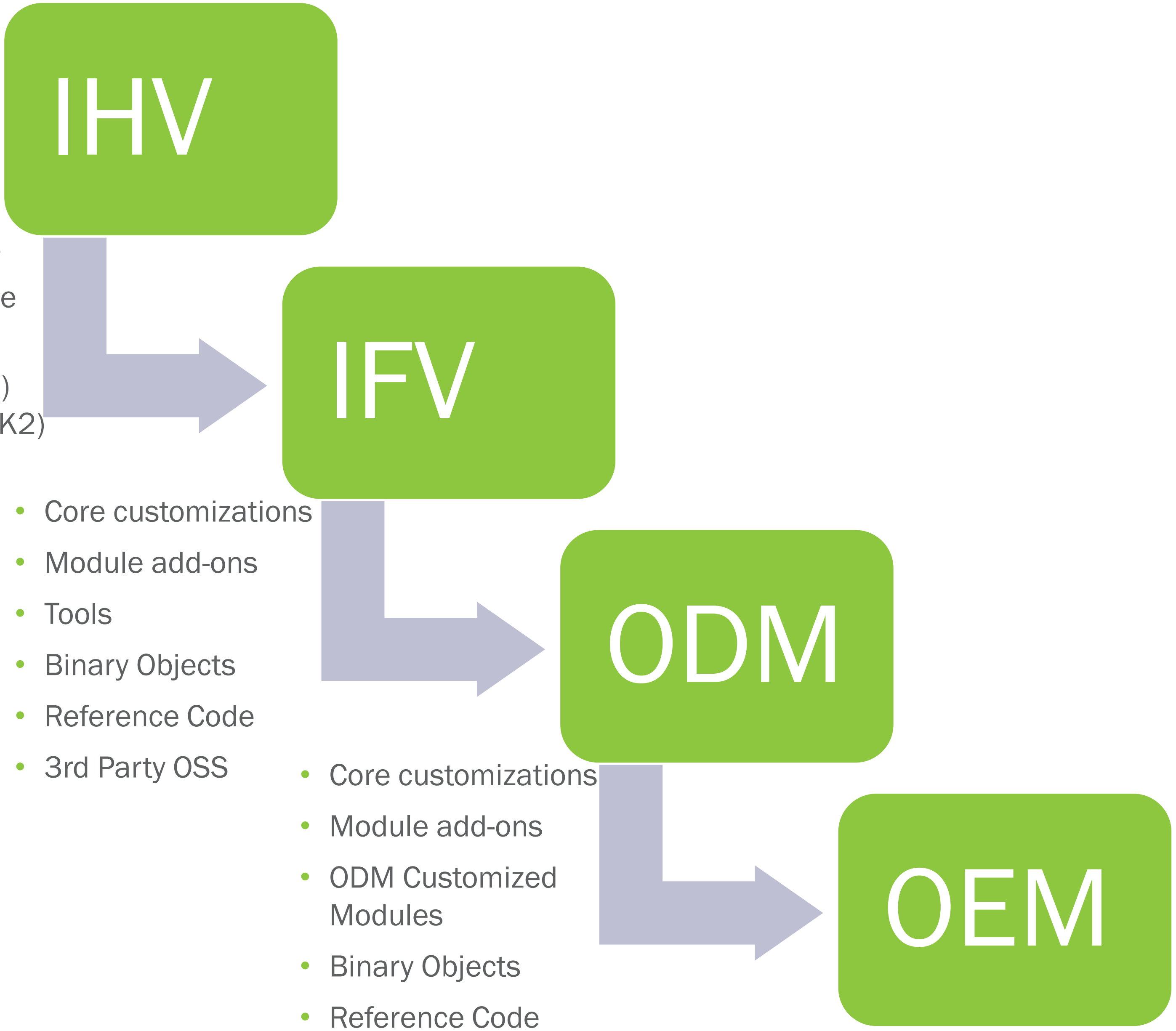
Risk Mitigation: Ripple20 – Treck IP stack

SBOM Capabilities

INVENTORY TRACKING	SOFTWARE DEPENDENCIES	PROVENANCE	PEDIGREE	VULNERABILITY STATUS	LICENSE ATTRIBUTION	INTEGRITY, AUTHENTICITY
– Component Name – Vendor Name – Version – Unique Identifier	– Ability to visualize dependencies with unidirectional acyclic graphs – Determine components are affected	– Software Origination Details	– Details of changes to software – Vulnerability remediations	– Provides the ability to detail the state of vulnerabilities in the product at the time the SBOM was created.	– Avoid copy-left issues – Facilitates license compliance	– Mechanisms are supported to ensure SBOM information is authentic.

Firmware Supply Chain Challenges

Connect. Collaborate. Accelerate.



- Binary Objects
- Reference code
- Open-source Software (OSS) (TianoCore EDK2)

- Core customizations
- Module add-ons
- Tools
- Binary Objects
- Reference Code
- 3rd Party OSS

- Core customizations
- Module add-ons
- ODM Customized Modules
- Binary Objects
- Reference Code
- 3rd Party OSS

Challenges

- Tools and processes still in nascent form
  - Universally adopted software naming convention– PURL?
- SCA challenges
- Patch management
- Vulnerability management
  - Needs to be modern and automated (no more spreadsheets and emails)
- How to begin such an effort, get traction, and build momentum?
- Ubiquity of SBOM - We need build tools that are just as capable of generating an SBOM for source code as they are capable of generate binaries from the code.
- How to handle transparency for binary objects?
  - How to get an SBOM that corresponds to the binary

Transparency via SBOM

Software traverses the supply chain in the form of source code and binaries. An SBOM ecosystem must support the ability to provide an SBOM for the binary or source code representation of the SW.

Consider the flowing approaches:

Method	Benefit	Drawback	Related
Store Complete SBOM in the binary	Not dependent on any other systems to derive complete SBOM	Adds size to the binary object	Embedding coSWID tags in the binary object files https://github.com/hughsie/python-uswid
Store a reference to an SBOM in the binary	Small size, easy to update	Need a system to extract SW IDs Need systems to facilitate fetching BOM for each SWID	Embedding coSWID tags in the binary object https://github.com/hughsie/python-uswid
Measured reference	Little to no size added to binary	Need a system to measure the binary Need a system to cross-reference the measurement with a DB of SWIDs. Need a system to facilitate fetching BOM for each SWID	Intel leverages TPM architecture to implement SBOM: https://uefi.org/node/4261

Strategy

Connect. Collaborate. Accelerate.

Open Compute Project®

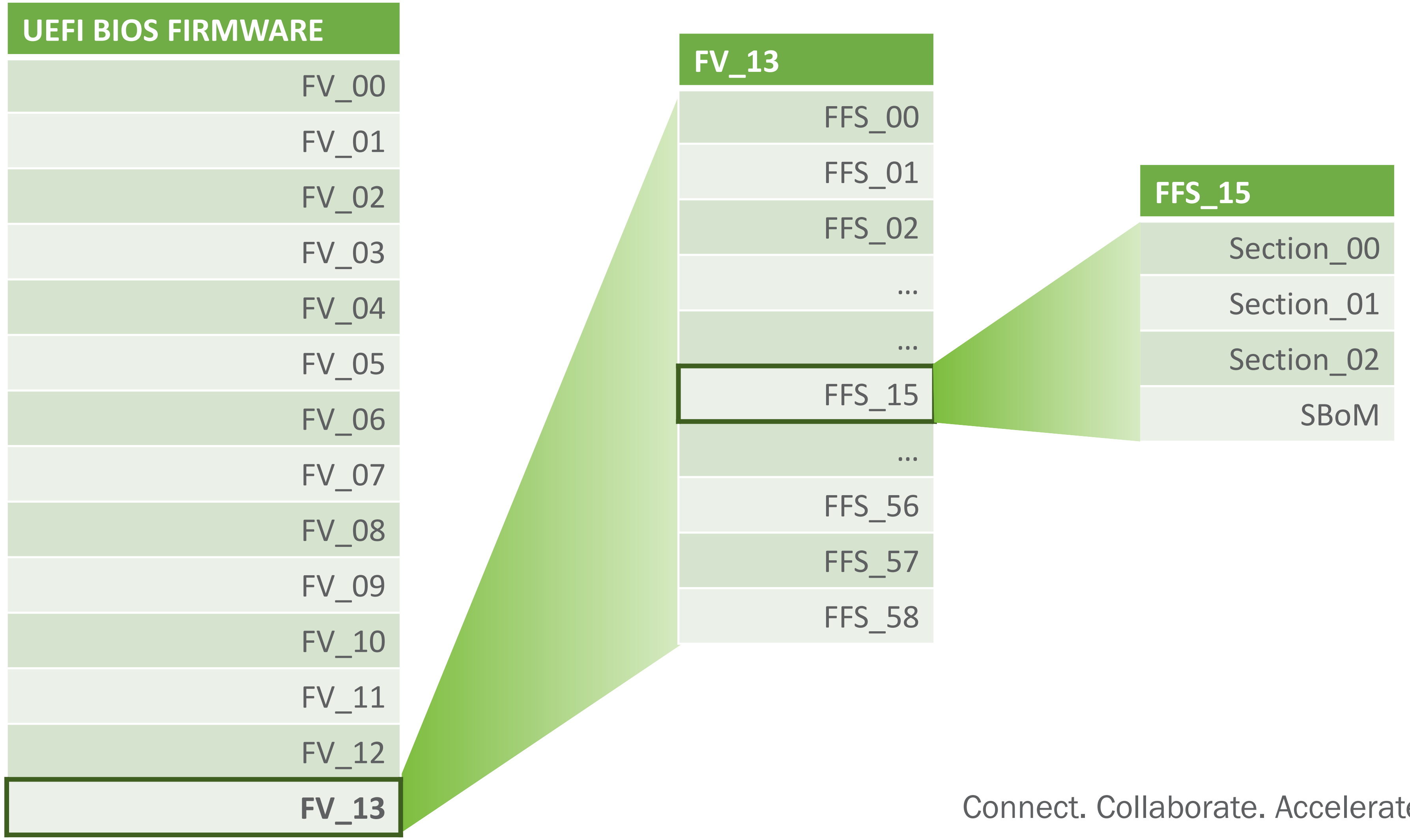
Strategy

- Crawl, Walk then Run

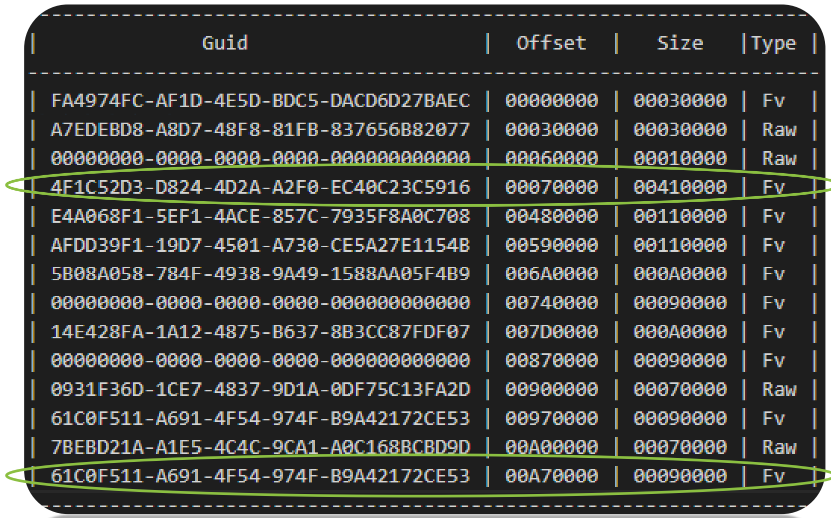
- Identify which use cases matter to the supply chain
  - Start with use cases needed by current organization
  - Create PoCs and socialize
  - Pull in supply chain partners to implement a broader industry wide PoC
    - Sync up on tooling/formats
    - Discover and prioritize use cases of supply chain partners

- Focus on the ability to accurately identify the ingredients in your FW first
  - Good SCA uses snippet checking to find traces of OSS followed by manual investigation to identify versions of that OSS
  - Need to modernize PSIRT/VMS

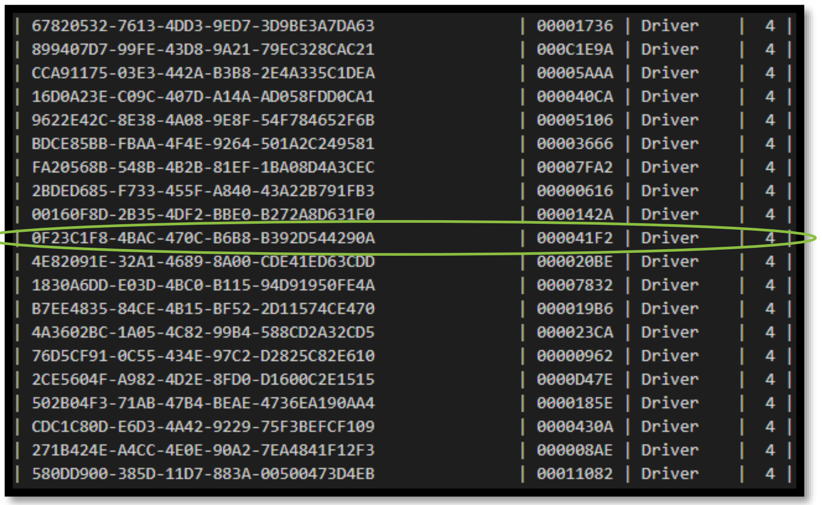
PoC: Embed SW IDs in a binary



Firmware Volume information

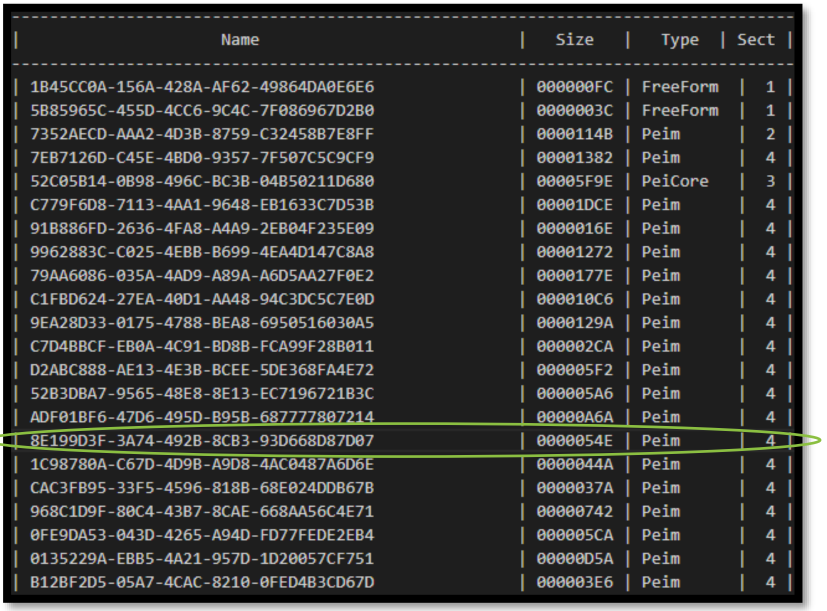


```
--------------------------------------------------------------------------
|                  Guid                  | Offset   |   Size   |Type |
--------------------------------------------------------------------------
| FA4974FC-AF1D-4E5D-BDC5-DACD6D27BAEC | 00000000 | 00030000 | Fv  |
| A7EDEBD8-A8D7-48F8-81FB-837656B82077 | 00030000 | 00030000 | Raw |
| 00000000-0000-0000-0000-000000000000 | 00060000 | 00010000 | Raw |
| 4F1C52D3-D824-4D2A-A2F0-EC40C23C5916 | 00070000 | 00410000 | Fv  |
| E4A068F1-5EF1-4ACE-857C-7935F8A0C708 | 00480000 | 00110000 | Fv  |
| AFDD39F1-19D7-4501-A730-CE5A27E1154B | 00590000 | 00110000 | Fv  |
| 5B08A058-784F-4938-9A49-1588AA05F4B9 | 006A0000 | 000A0000 | Fv  |
| 00000000-0000-0000-0000-000000000000 | 00740000 | 00090000 | Fv  |
| 14E428FA-1A12-4875-B637-8B3CC87FDF07 | 007D0000 | 000A0000 | Fv  |
| 00000000-0000-0000-0000-000000000000 | 00870000 | 00090000 | Fv  |
| 0931F36D-1CE7-4837-9D1A-0DF75C13FA2D | 00900000 | 00070000 | Raw |
| 61C0F511-A691-4F54-974F-B9A42172CE53 | 00970000 | 00090000 | Fv  |
| 7BEBD21A-A1E5-4C4C-9CA1-A0C168BCBD9D | 00A00000 | 00070000 | Raw |
| 61C0F511-A691-4F54-974F-B9A42172CE53 | 00A70000 | 00090000 | Fv  |
--------------------------------------------------------------------------
```



```
| 67820532-7613-4DD3-9ED7-3D9BE3A7DA63                 | 00001736 | Driver   |  4 |
| 899407D7-99FE-43D8-9A21-79EC328CAC21                 | 000C1E9A | Driver   |  4 |
| CCA91175-03E3-442A-B3B8-2E4A335C1DEA                 | 00005AAA | Driver   |  4 |
| 16D0A23E-C09C-407D-A14A-AD058FDD0CA1                 | 000040CA | Driver   |  4 |
| 9622E42C-8E38-4A08-9E8F-54F784652F6B                 | 00005106 | Driver   |  4 |
| BDCE85BB-FBAA-4F4E-9264-501A2C249581                 | 00003666 | Driver   |  4 |
| FA20568B-548B-4B2B-81EF-1BA08D4A3CEC                 | 00007FA2 | Driver   |  4 |
| 2BDED685-F733-455F-A840-43A22B791FB3                 | 00000616 | Driver   |  4 |
| 00160F8D-2B35-4DF2-BBE0-B272A8D631F0                 | 0000142A | Driver   |  4 |
| 0F23C1F8-4BAC-470C-B6B8-B392D544290A                 | 000041F2 | Driver   |  4 |
| 4E82091E-32A1-4689-8A00-CDE41ED63CDD                 | 000020BE | Driver   |  4 |
| 1830A6DD-E03D-4BC0-B115-94D91950FE4A                 | 00007832 | Driver   |  4 |
| B7EE4835-84CE-4B15-BF52-2D11574CE470                 | 000019B6 | Driver   |  4 |
| 4A3602BC-1A05-4C82-99B4-588CD2A32CD5                 | 000023CA | Driver   |  4 |
| 76D5CF91-0C55-434E-97C2-D2825C82E610                 | 00000962 | Driver   |  4 |
| 2CE5604F-A982-4D2E-8FD0-D1600C2E1515                 | 0000D47E | Driver   |  4 |
| 502B04F3-71AB-47B4-BEAE-4736EA190AA4                 | 0000185E | Driver   |  4 |
| CDC1C80D-E6D3-4A42-9229-75F3BEFCF109                 | 0000430A | Driver   |  4 |
| 271B424E-A4CC-4E0E-90A2-7EA4841F12F3                 | 000008AE | Driver   |  4 |
| 580DD900-385D-11D7-883A-00500473D4EB                 | 00011082 | Driver   |  4 |
```

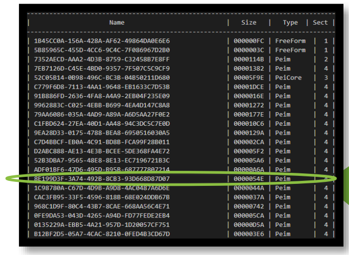
Firmware File System information (DXE)
In Nested FV [Compressed]



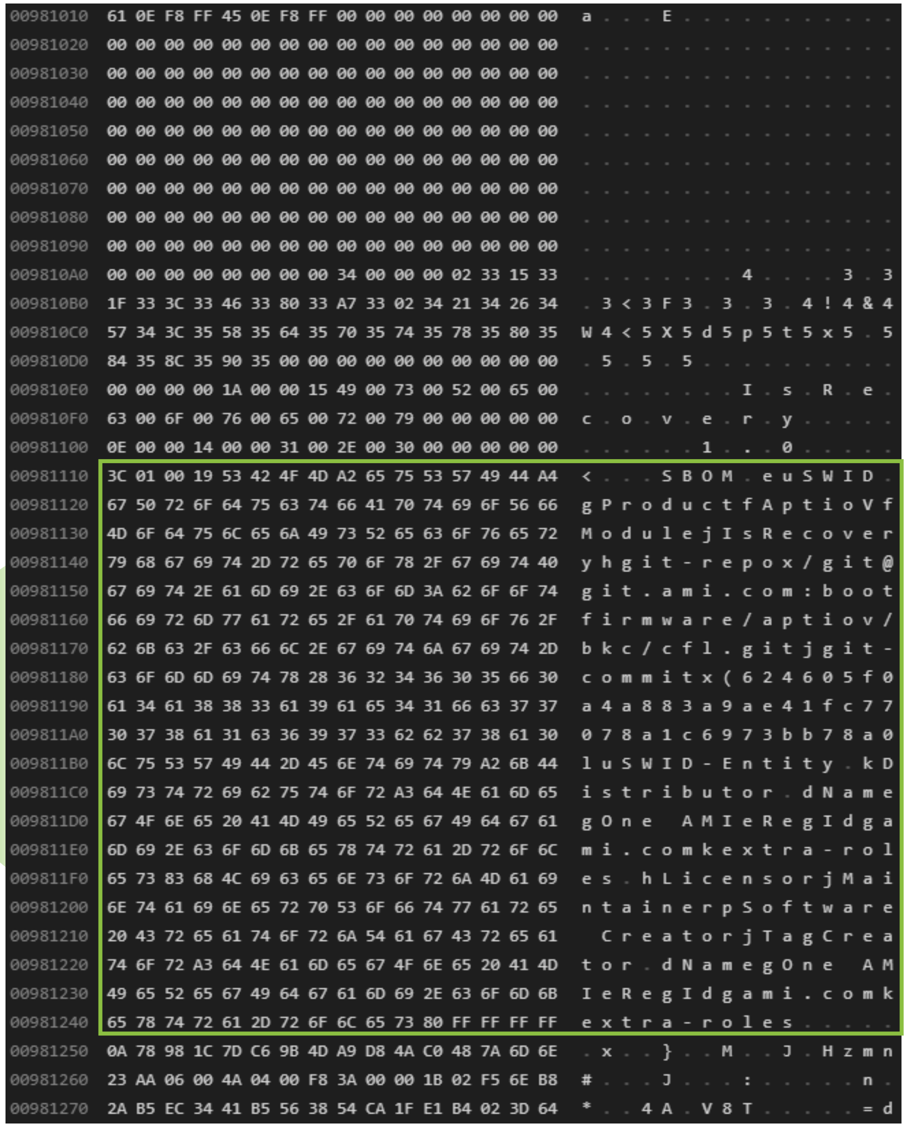
```
-------------------------------------------------------------------------------------
|                         Name                         |   Size   |   Type   | Sect |
-------------------------------------------------------------------------------------
| 1B45CC0A-156A-428A-AF62-49864DA0E6E6                 | 000000FC | FreeForm |  1 |
| 5B85965C-455D-4CC6-9C4C-7F086967D2B0                 | 0000003C | FreeForm |  1 |
| 7352AECD-AAA2-4D3B-8759-C32458B7E8FF                 | 0000114B | Peim     |  2 |
| 7EB7126D-C45E-4BD0-9357-7F507C5C9CF9                 | 00001382 | Peim     |  4 |
| 52C05B14-0B98-496C-BC3B-04B50211D680                 | 00005F9E | PeiCore  |  3 |
| C779F6D8-7113-4AA1-9648-EB1633C7D53B                 | 00001DCE | Peim     |  4 |
| 91B886FD-2636-4FA8-A4A9-2EB04F235E09                 | 0000016E | Peim     |  4 |
| 9962883C-C025-4EBB-B699-4EA4D147C8A8                 | 00001272 | Peim     |  4 |
| 79AA6086-035A-4AD9-A89A-A6D5AA27F0E2                 | 0000177E | Peim     |  4 |
| C1FBD624-27EA-40D1-AA48-94C3DC5C7E0D                 | 000010C6 | Peim     |  4 |
| 9EA28D33-0175-4788-BEA8-6950516030A5                 | 0000129A | Peim     |  4 |
| C7D4BBCF-EB0A-4C91-BD8B-FCA99F28B011                 | 000002CA | Peim     |  4 |
| D2ABC888-AE13-4E3B-BCEE-5DE368FA4E72                 | 000005F2 | Peim     |  4 |
| 52B3DBA7-9565-48E8-8E13-EC7196721B3C                 | 000005A6 | Peim     |  4 |
| ADF01BF6-47D6-495D-B95B-687777807214                 | 00000A6A | Peim     |  4 |
| 8E199D3F-3A74-492B-8CB3-93D668D87D07                 | 0000054E | Peim     |  4 |
| 1C98780A-C67D-4D9B-A9D8-4AC0487A6D6E                 | 0000044A | Peim     |  4 |
| CAC3FB95-33F5-4596-818B-68E024DDB67B                 | 0000037A | Peim     |  4 |
| 968C1D9F-80C4-43B7-8CAE-668AA56C4E71                 | 00000742 | Peim     |  4 |
| 0FE9DA53-043D-4265-A94D-FD77FEDE2EB4                 | 000005CA | Peim     |  4 |
| 0135229A-EBB5-4A21-957D-1D20057CF751                 | 00000D5A | Peim     |  4 |
| B12BF2D5-05A7-4CAC-8210-0FED4B3CD67D                 | 000003E6 | Peim     |  4 |
```

Firmware File System information (PEI)

PEI



```
| Name                                  | Size     | Type     | Sect |
------------------------------------------------------------------------
| 1B45CC0A-156A-428A-AF62-49864DA0E6E6  | 000000FC | FreeForm |  1 |
| 5B85965C-455D-4CC6-9C4C-7F086967D2B0  | 0000003C | FreeForm |  1 |
| 7352AECD-AAA2-4D3B-8759-C32458B7E8FF  | 0000114B | Peim     |  2 |
| 7EB7126D-C45E-4BD0-9357-7F507C5C9CF9  | 00001382 | Peim     |  4 |
| 52C05B14-0B98-496C-BC3B-04B50211D680  | 00005F9E | PeiCore  |  3 |
| C779F6D8-7113-4AA1-9648-EB1633C7D53B  | 00001DCE | Peim     |  4 |
| 91B886FD-2636-4FA8-A4A9-2EB04F235E09  | 0000016E | Peim     |  4 |
| 9962883C-C025-4EBB-B699-4EA4D147C8A8  | 00001272 | Peim     |  4 |
| 79AA6086-035A-4AD9-A89A-A6D5AA27F0E2  | 0000177E | Peim     |  4 |
| C1FBD624-27EA-40D1-AA48-94C3DC5C7E0D  | 000010C6 | Peim     |  4 |
| 9EA28D33-0175-4788-BEA8-6950516030A5  | 0000129A | Peim     |  4 |
| C7D4BBCF-EB0A-4C91-BD8B-FCA99F28B011  | 000002CA | Peim     |  4 |
| D2ABC888-AE13-4E3B-BCEE-5DE368FA4E72  | 000005F2 | Peim     |  4 |
| 52B3DBA7-9565-48E8-8E13-EC7196721B3C  | 000005A6 | Peim     |  4 |
| ADF01BF6-47D6-495D-B95B-687777807214  | 00000A6A | Peim     |  4 |
| 8E199D3F-3A74-492B-8CB3-93D668D87D07  | 0000054E | Peim     |  4 |
| 1C98780A-C67D-4D9B-A9D8-4AC0487A6D6E  | 0000044A | Peim     |  4 |
| CAC3FB95-33F5-4596-818B-68E024DDB67B  | 0000037A | Peim     |  4 |
| 968C1D9F-80C4-43B7-8CAE-668AA56C4E71  | 00000742 | Peim     |  4 |
| 0FE9DA53-043D-4265-A94D-FD77FEDE2EB4  | 000005CA | Peim     |  4 |
| 0135229A-EBB5-4A21-957D-1D20057CF751  | 00000D5A | Peim     |  4 |
| B12BF2D5-05A7-4CAC-8210-0FED4B3CD67D  | 000003E6 | Peim     |  4 |
```



```
00981010  61 0E F8 FF 45 0E F8 FF 00 00 00 00 00 00 00 00  a . . . E . . . . . . . . . . .
00981020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
00981090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
009810A0  00 00 00 00 00 00 00 00 34 00 00 00 02 33 15 33  . . . . . . . . 4 . . . . 3 . 3
009810B0  1F 33 3C 33 46 33 80 33 A7 33 02 34 21 34 26 34  . 3 < 3 F 3 . 3 . 3 . 4 ! 4 & 4
009810C0  57 34 3C 35 58 35 64 35 70 35 74 35 78 35 80 35  W 4 < 5 X 5 d 5 p 5 t 5 x 5 . 5
009810D0  84 35 8C 35 90 35 00 00 00 00 00 00 00 00 00 00  . 5 . 5 . 5 . . . . . . . . . .
009810E0  00 00 00 00 1A 00 00 15 49 00 73 00 52 00 65 00  . . . . . . . . I . s . R . e .
009810F0  63 00 6F 00 76 00 65 00 72 00 79 00 00 00 00 00  c . o . v . e . r . y . . . . .
00981100  0E 00 00 14 00 00 31 00 2E 00 30 00 00 00 00 00  . . . . . . 1 . . . 0 . . . . .
00981110  3C 01 00 19 53 42 4F 4D A2 65 75 53 57 49 44 A4  < . . . S B O M . e u S W I D .
00981120  67 50 72 6F 64 75 63 74 66 41 70 74 69 6F 56 66  g P r o d u c t f A p t i o V f
00981130  4D 6F 64 75 6C 65 6A 49 73 52 65 63 6F 76 65 72  M o d u l e j I s R e c o v e r
00981140  79 68 67 69 74 2D 72 65 70 6F 78 2F 67 69 74 40  y h g i t - r e p o x / g i t @
00981150  67 69 74 2E 61 6D 69 2E 63 6F 6D 3A 62 6F 6F 74  g i t . a m i . c o m : b o o t
00981160  66 69 72 6D 77 61 72 65 2F 61 70 74 69 6F 76 2F  f i r m w a r e / a p t i o v /
00981170  62 6B 63 2F 63 66 6C 2E 67 69 74 6A 67 69 74 2D  b k c / c f l . g i t j g i t -
00981180  63 6F 6D 6D 69 74 78 28 36 32 34 36 30 35 66 30  c o m m i t x ( 6 2 4 6 0 5 f 0
00981190  61 34 61 38 38 33 61 39 61 65 34 31 66 63 37 37  a 4 a 8 8 3 a 9 a e 4 1 f c 7 7
009811A0  30 37 38 61 31 63 36 39 37 33 62 62 37 38 61 30  0 7 8 a 1 c 6 9 7 3 b b 7 8 a 0
009811B0  6C 75 53 57 49 44 2D 45 6E 74 69 74 79 A2 6B 44  l u S W I D - E n t i t y . k D
009811C0  69 73 74 72 69 62 75 74 6F 72 A3 64 4E 61 6D 65  i s t r i b u t o r . d N a m e
009811D0  67 4F 6E 65 20 41 4D 49 65 52 65 67 49 64 67 61  g O n e   A M I e R e g I d g a
009811E0  6D 69 2E 63 6F 6D 6B 65 78 74 72 61 2D 72 6F 6C  m i . c o m k e x t r a - r o l
009811F0  65 73 83 68 4C 69 63 65 6E 73 6F 72 6A 4D 61 69  e s . h L i c e n s o r j M a i
00981200  6E 74 61 69 6E 65 72 70 53 6F 66 74 77 61 72 65  n t a i n e r p S o f t w a r e
00981210  20 43 72 65 61 74 6F 72 6A 54 61 67 43 72 65 61    C r e a t o r j T a g C r e a
00981220  74 6F 72 A3 64 4E 61 6D 65 67 4F 6E 65 20 41 4D  t o r . d N a m e g O n e   A M
00981230  49 65 52 65 67 49 64 67 61 6D 69 2E 63 6F 6D 6B  I e R e g I d g a m i . c o m k
00981240  65 78 74 72 61 2D 72 6F 6C 65 73 80 FF FF FF FF  e x t r a - r o l e s . . . . .
00981250  0A 78 98 1C 7D C6 9B 4D A9 D8 4A C0 48 7A 6D 6E  . x . . } . . M . . J . H z m n
00981260  23 AA 06 00 4A 04 00 F8 3A 00 00 1B 02 F5 6E B8  # . . . J . . . : . . . . . n .
00981270  2A B5 EC 34 41 B5 56 38 54 CA 1F E1 B4 02 3D 64  * . . 4 A . V 8 T . . . . . = d
```

SBOM Information

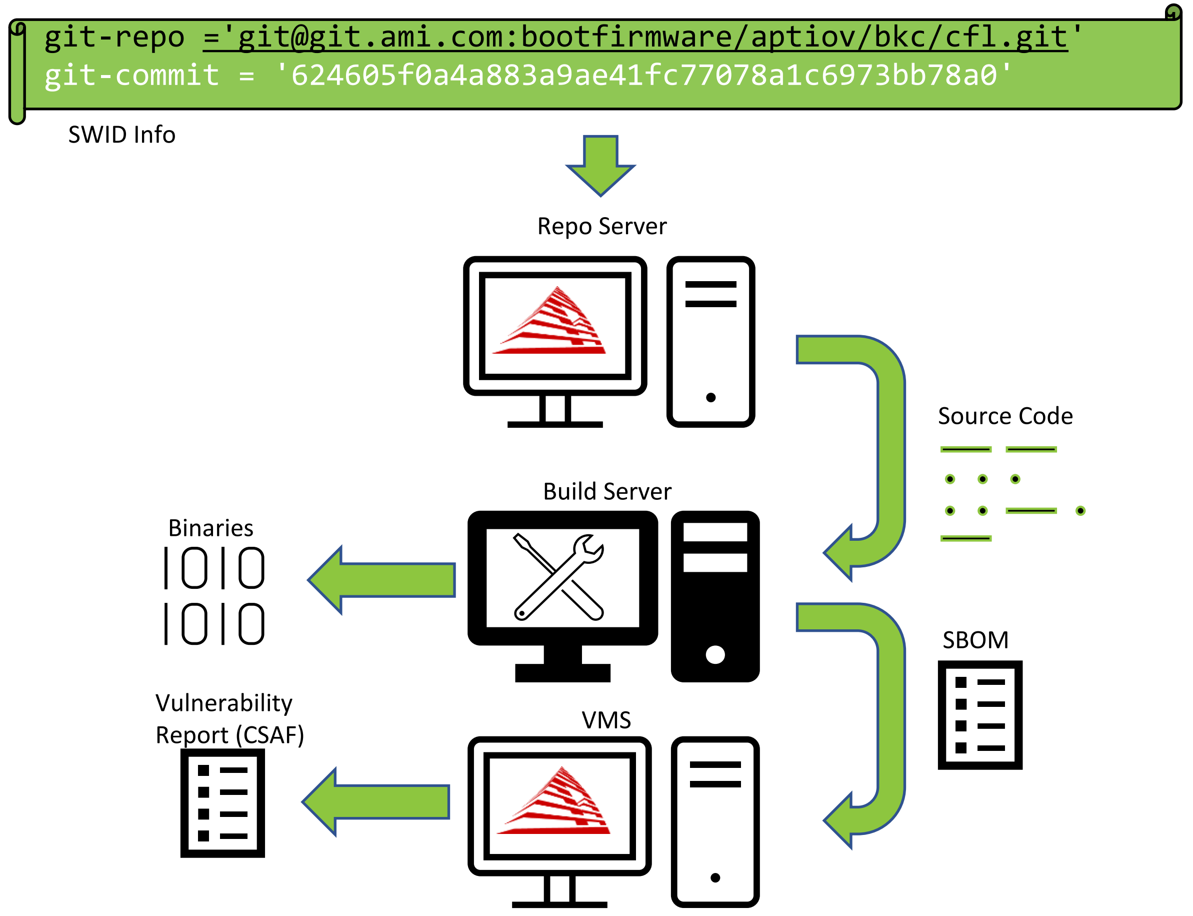
[uSWID]
Product = 'Aptio'
Module = 'IsRecovery'
git-repo =
'git@git.ami.com:bootfirmware/aptiov/bkc/cfl.git'
git-commit =
'624605f0a4a883a9ae41fc77078a1c6973bb78a0'

[uSWID-Entity]
[uSWID-Entity.Distributor]
Name = 'One AMI'
RegId = 'ami.com'
extra-roles = ['Licensor', 'Maintainer', 'Software Creator']

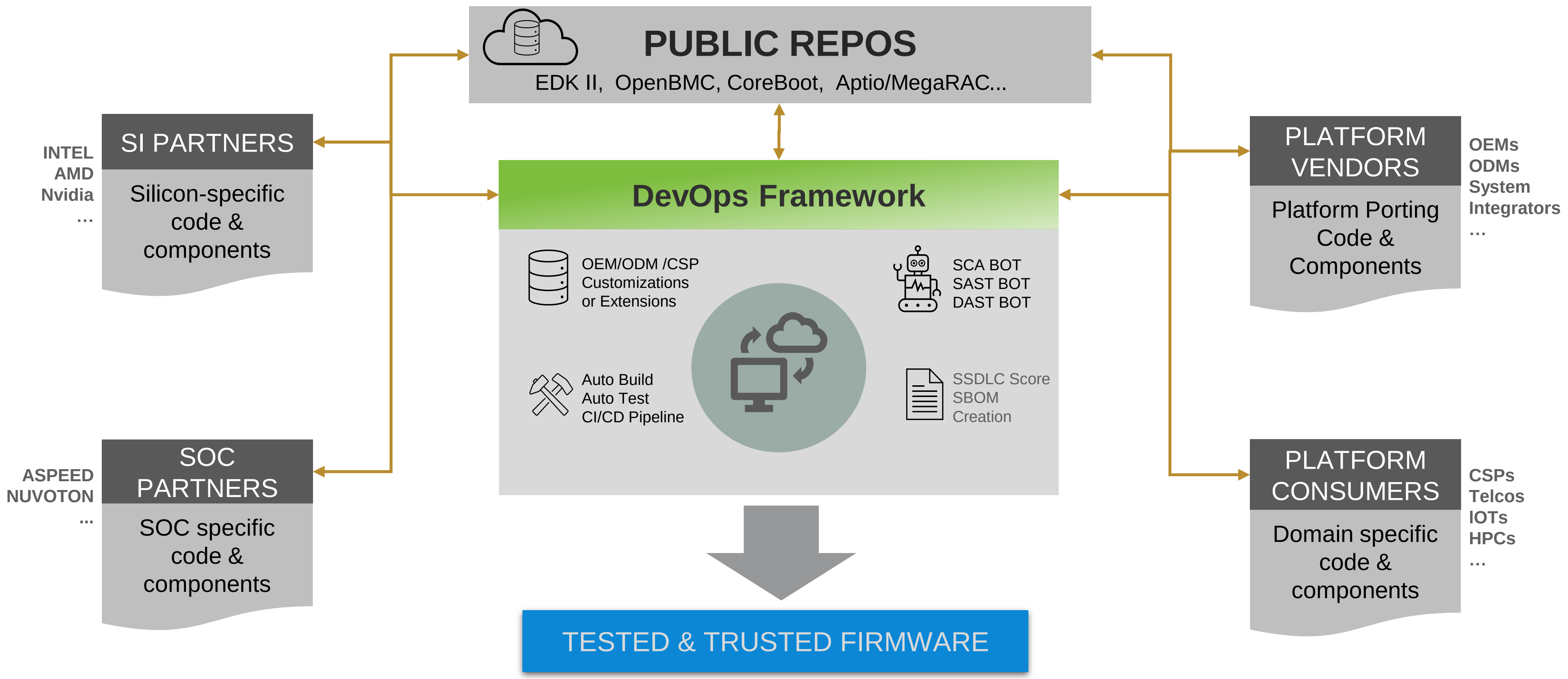
[uSWID-Entity.TagCreator]
Name = 'One AMI'
RegId = 'ami.com'
extra-roles = []

Connect. Collaborate. Accelerate.

Advertisement and Discovery

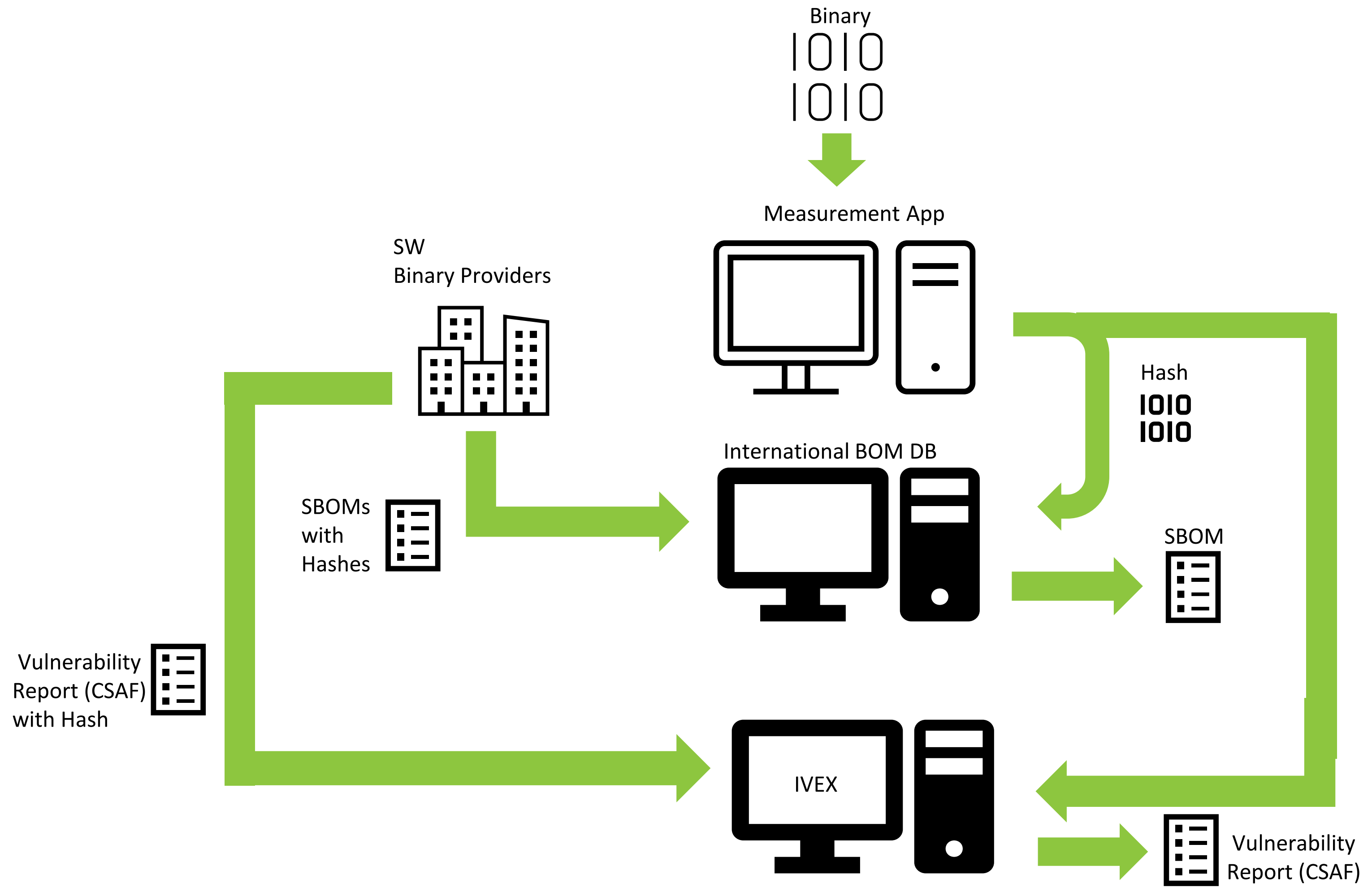

```
git-repo ='git@git.ami.com:bootfirmware/aptiov/bkc/cfl.git'
git-commit = '624605f0a4a883a9ae41fc77078a1c6973bb78a0'
```

Eco-centric Automation



Connect. Collaborate. Accelerate.

An Open SBOM Ecosystem



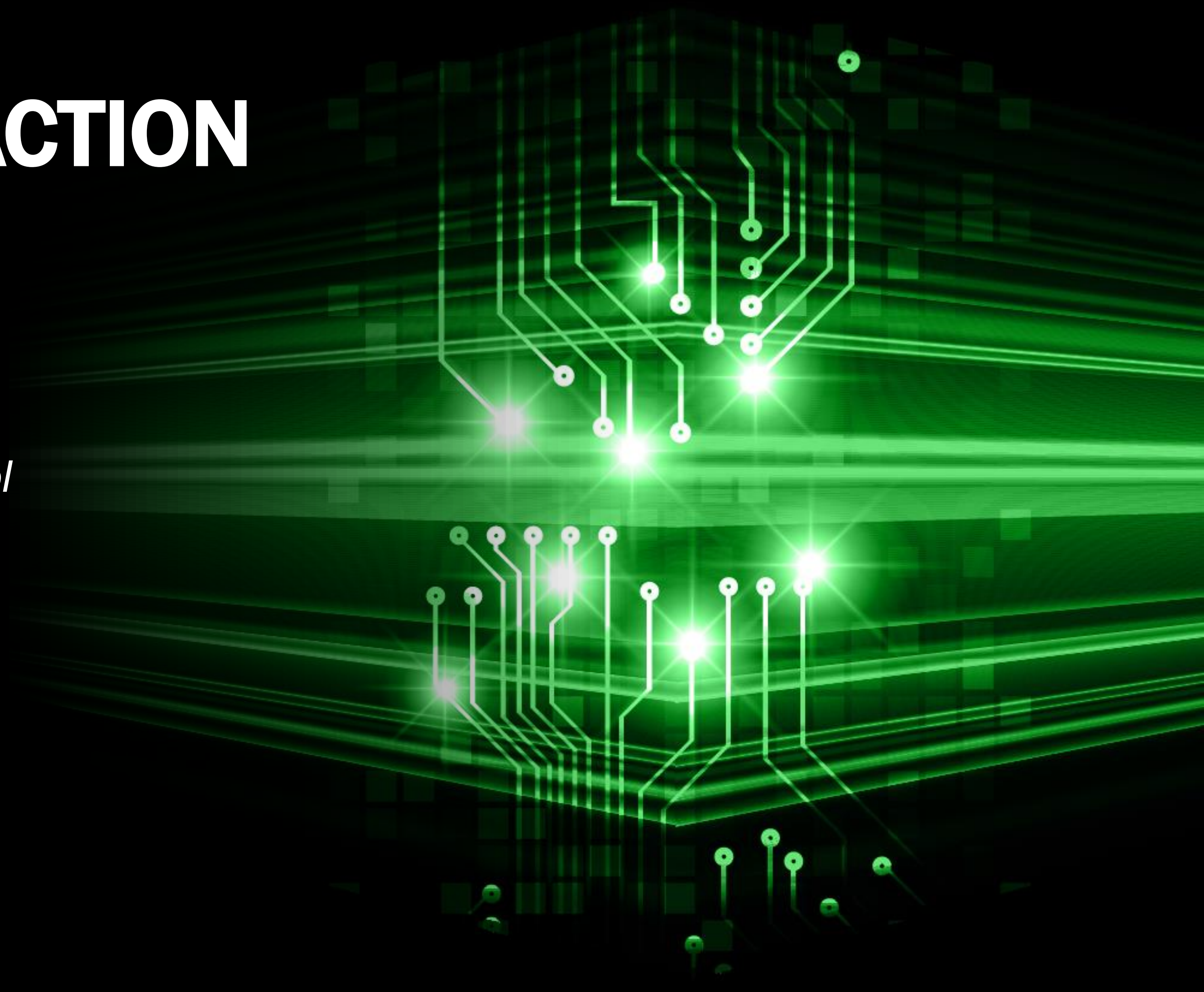
OPEN Compute Project®

CALL TO ACTION

Build an expanded PoC

- *Cross-vendor SBOM consumption tool*
  - ✓ *Silicon Vendors (IHV)*
  - ✓ *IFV*
  - ✓ *ODM*
  - ✓ *OEM*
  - ✓ *Point of Use (PoU)*

Contact AMI (ami.com/contact)



Resources

Executive Order Related: Why we must do it:

- https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
- https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Ripple20: Why we should do it.

- https://www.jsof-tech.com/disclosures/ripple20/

Who is using SBOM and why:

- https://linuxfoundation.org/wp-content/uploads/LFResearch_SBOM_Report_final.pdf

Good intro to SBOM use cases:

- OWASP SBOM Use Cases: https://www.youtube.com/watch?v=PNYyMpUey7Y

Good info on industry wide proof-of-concepts and much more generic SBOM info

- https://www.cisa.gov/cisa-sbom-rama

Methods/Tools for associating SBOMs with binaries:

- https://github.com/hughsie/python-uswid (LVFS/Redhat/Richard Hughes' embedded coSWID tags solution)
- https://www.ietf.org/archive/id/draft-ietf-sacm-coswid-21.txt
- https://uefi.org/node/4261 (Intel's approach with TPM/RIM)

Proof of concept

- https://toml.io/en/v1.0.0
- https://en.wikipedia.org/wiki/CBOR
- https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf (Advertisement and Discovery)

VEX

- https://www.ntia.doc.gov/files/ntia/publications/framing_2021-04-29_002.pdf

SBOM Tooling Info:

- https://cyclonedx.org/tool-center/
- https://spdx.dev/resources/tools/

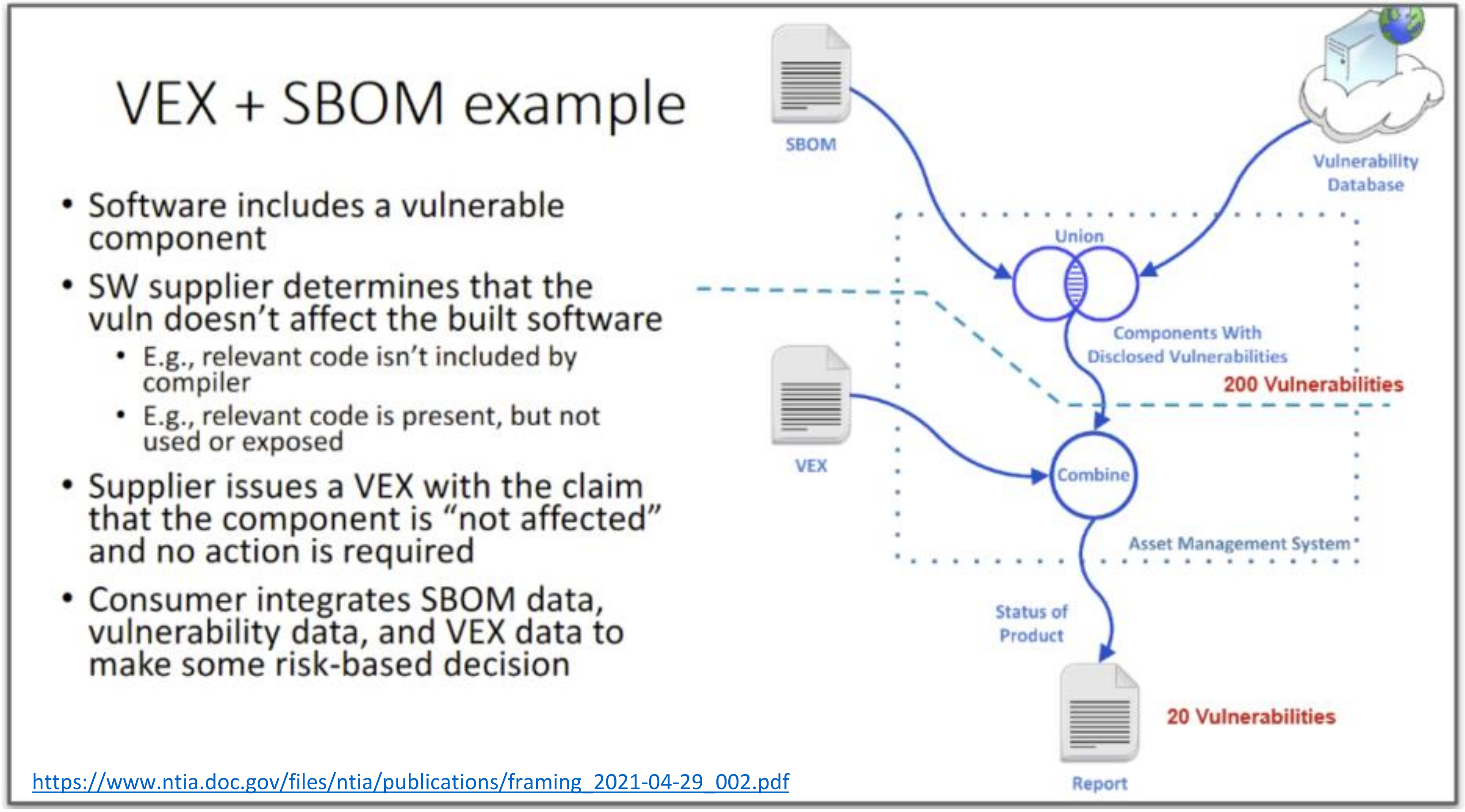
Thank you!

OPEN Compute Project®

Connect. Collaborate. Accelerate.

Backup

VEX



VEX + SBOM example

- Software includes a vulnerable component
- SW supplier determines that the vuln doesn't affect the built software
  - E.g., relevant code isn't included by compiler
  - E.g., relevant code is present, but not used or exposed
- Supplier issues a VEX with the claim that the component is "not affected" and no action is required
- Consumer integrates SBOM data, vulnerability data, and VEX data to make some risk-based decision

https://www.ntia.doc.gov/files/ntia/publications/framing_2021-04-29_002.pdf