Examples based on the Use Cases from Information Sharing Architecture (ISA) Access Control Specification (ACS) – version 3.0a

Section 5 of Information Sharing Architecture (ISA) Access Control Specification (ACS) version 3.0a contains five use cases for ACS data markings. This document contains examples of these use cases expressed in STIX as defined in [ref] [ref]

# Use Case 1

{

"id": "bundle--15067de5-05b6-4330-8104-45da359c2d2a",

"objects": [

{

"created": "2020-06-18T00:00:00Z",

"definition": {

"control\_set": {

"classification": "TS",

"entity": ["GOV", "CTR", "MIL"],

"shareability": ["NCC"]

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-3bda2f6e-cedc-4c0f-a756-c03d6b586917",

"name": "Use Case 1: Access Granted to Cybersecurity Data",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny",

"responsible\_entity\_custodian": "USA.NSA",

"sep\_version": 1

},

"definition\_type": "x-isa-acs-3-0",

"id": "marking-definition--20864905-06a0-47be-a04c-2164af17d635",

"type": "marking-definition"

}

],

"type": "bundle"

}

# Use Case 2

{

"type": "bundle",

"id": "bundle--5be1c5b5-98ee-408e-918c-2ead90bc8014",

"objects": [

{

"type": "marking-definition",

"created": "2020-06-18T00:00:00Z",

"definition\_type": "x-isa-acs-3-0",

"definition": {

"access\_privilege": [

{

"privilege\_action": "INTEL",

"privilege\_scope": {

"entity": ["ALL"],

"permitted\_nationalities": ["ALL"],

"permitted\_organizations": ["ALL"],

"shareability": ["ALL"]

},

"rule\_effect": "permit"

},

{

"privilege\_action": "DSPLY",

"privilege\_scope": {

"entity": ["ALL"],

"permitted\_nationalities": ["ALL"],

"permitted\_organizations": ["ALL"],

"shareability": ["ALL"]

},

"rule\_effect": "permit"

},

{

"privilege\_action": "REQUEST",

"privilege\_scope": {

"entity": ["ALL"],

"permitted\_nationalities": ["ALL"],

"permitted\_organizations": ["ALL"],

"shareability": ["ALL"]

},

"rule\_effect": "permit"

}

],

"control\_set": {

"classification": "U",

"formal\_determination": ["FOUO"]

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-76342cc9-1440-4031-84a3-d498c404cab3",

"name": "Use Case 2: Access Privilege",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",

"responsible\_entity\_custodian": "USA.DOJ.FBI",

"sep\_version": 1

},

"id": "marking-definition--6010b3f4-a603-4d3b-9098-8708cdbe151b"

}

]

}

# Use Case 3

{

"type": "bundle",

"id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",

"objects": [

{

"type": "marking-definition",

"created": "2020-06-18T00:00:00Z",

"definition\_type": "x-isa-acs-3-0",

"definition": {

"control\_set": {

"classification": "S"

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-a526c69f-1468-4f4e-96eb-cdbf302cc0e3",

"name": "Use Case 3: PUBREL and Portion Marking - S",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit",

"responsible\_entity\_custodian": "USA.DHS",

"sep\_version": 1

},

"id": "marking-definition--e3896452-4dcf-4e19-a571-8571c1c530a2"

},

{

"type": "marking-definition",

"id": "marking-definition--d0038fa3-d4db-460b-813d-191917213910",

"created": "2020-06-18T00:00:00Z",

"definition\_type": "x-isa-acs-3-0",

"definition": {

"control\_set": {

"classification": "U",

"formal\_determination": ["PUBREL"]

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-2db30d2d-036c-4631-a057-bd85b189adee",

"name": "Use Case 3: PUBREL and Portion Marking - U",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",

"public\_release": {

"released\_by": "Authority",

"released\_on": "2020-01-01T00:00:00Z"

},

"responsible\_entity\_custodian": "USA.DHS",

"sep\_version": 1

}

},

{

"object\_marking\_refs": [

"marking-definition--d0038fa3-d4db-460b-813d-191917213910"

],

"id": "ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd",

"type": "ipv4-addr",

"value": "198.51.100.3"

},

{

"type": "threat-actor",

"spec\_version": "2.1",

"id": "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created": "2016-04-06T20:03:48.000Z",

"modified": "2016-04-06T20:03:48.000Z",

"threat\_actor\_types": [ "nation\_state"],

"name": "Evil Republic Div 37",

"sophistication": "expert",

"resource\_level": "government",

"primary\_motivation": "organizational-gain",

"object\_marking\_refs": [

"marking-definition--e3896452-4dcf-4e19-a571-8571c1c530a2"

]

},

{

"type": "report",

"spec\_version": "2.1",

"id": "report--eff11c91-12da-4bec-ac82-285d1efc0cf6",

"created": "2020-06-18T00:00:00Z",

"modified": "2020-06-18T00:00:00Z",

"name": "Use Case 3: PUBREL and Portion Marking",

"published": "2020-07-19T00:00:00Z",

"report\_types": [ "threat-actor"],

"object\_refs": [

"marking-definition--e3896452-4dcf-4e19-a571-8571c1c530a2",

"marking-definition--d0038fa3-d4db-460b-813d-191917213910",

"ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd",

"threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"

]

}

]

}

# Use Case 4

{

"id": "bundle--0a2277ac-a785-4c11-b691-582293ea9eb1",

"objects": [

{

"created": "2020-06-18T00:00:00Z",

"definition": {

"control\_set": {

"classification": "U",

"entity": [ "MIL", "CTR", "GOV", "SVR", "SVC", "DEV", "NET"],

"permitted\_organizations": ["USA.USG"]

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-6b142579-f21c-4199-865c-207d9df7313c",

"name": "Use Case 4: Analytic NPE",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",

"responsible\_entity\_custodian": "USA.DOD.USCYBERCOM-JOC",

"sep\_version": 1

},

"definition\_type": "x-isa-acs-3-0",

"id": "marking-definition--ff7043e7-b1c9-4115-8bfc-79db1bed6862",

"type": "marking-definition"

}

],

"type": "bundle"

}

# Use Case 5

{

"id": "bundle--bfcf564a-6981-4000-8e8b-1cb42d26195a",

"objects": [

{

"created": "2020-06-18T00:00:00Z",

"definition": {

"control\_set": {

"classification": "U",

"entity": [ "MIL", "CTR", "GOV"],

"permitted\_organizations": ["USA.USG", "USA.SLTT"],

"sensitivity": ["LES"]

},

"create\_date\_time": "2018-05-27T14:10:26.723Z",

"identifier": "isa:guide.19001.ACS3-6b142579-f21c-4199-865c-207d9df7313c",

"name": "Use Case 5: Access Denied to Law Enforcement Data",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit",

"responsible\_entity\_custodian": "USA.DOJ.FBI",

"sep\_version": 1

},

"definition\_type": "x-isa-acs-3-0",

"id": "marking-definition--ff7043e7-b1c9-4115-8bfc-79db1bed6862",

"type": "marking-definition"

}

],

"type": "bundle"

}