



Intellectual Property Working Group (IPWG)

Requirements Document

Version 1.0

Publish Date: 25 November 2013

Prepared by: TSCP Intellectual Property Working Group (IPWG)

Copyright © 2013 Transglobal Secure Collaboration Participation Inc.

All rights reserved.

Terms and Conditions

Transglobal Secure Collaboration Participation, Inc. (TSCP) is a consortium comprising a number of commercial and government members (as further specified at <http://www.tscp.org>) (each a “TSCP Member”). This specification was developed and is being released under this open source license by TSCP.

Use of this specification is subject to the disclaimers and limitations described below. By using this specification, you (the user) agree to and accept the following terms and conditions:

1. This specification may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from or otherwise modify this specification. Redistribution and use of this specification, without modification, is permitted provided that the following conditions are met:

- Redistributions of this specification must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- TSCP’s name may not be used to endorse or promote products or services derived from this specification without specific prior written permission.

2. The use of technology described in or implemented in accordance with this specification may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS SPECIFICATION IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TSCP AND EACH TSCP MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER TSCP NOR ANY TSCP MEMBER WARRANTS (A) THAT THIS SPECIFICATION IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS SPECIFICATION, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF TSCP OR ANY THIRD PARTY.

4. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS SPECIFICATION, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS SPECIFICATION, THE USER WAIVES ANY SUCH CLAIM AGAINST TSCP OR ANY TSCP MEMBER RELATING TO THE USE OF THIS SPECIFICATION. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS SPECIFICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. TSCP reserves the right to modify or amend this specification at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this specification has been superseded by a later version or a different specification.

6. These terms and conditions will be interpreted and governed by the laws of the State of Delaware without regard to its conflict of laws and rules. Any party asserting any claims related to this specification irrevocably consents to the personal jurisdiction of the U.S. District Court for the District of Delaware and to any state court located in such district of the State of Delaware and waives any objections to the venue of such court.

Document Contributors:

Member Name	Member Company
Hayes, Crystal	The Boeing Company
Tolbert, John	The Boeing Company
Skedd, Richard	BAE Systems
Dupre, Florence	EADS
Smith, Martin	U.S. Department of Homeland Security

TABLE OF CONTENTS

1. Introduction	1
1.1 Purpose	1
1.2 Overview of Intellectual Property	1
2. Intellectual Property Business Scenarios	2
2.1 Business Scenario 1: Proprietary Information Agreement (PIA) Implementation Process.....	3
2.2 Business Scenario 2: Collaborative Agreements	8
2.3 Business Scenario 3: Sub-Tier Supplier Agreements.....	12
3. IP Access Authorization Flow.....	16
4. Requirements.....	18
4.1 Process Steps - Requirements	18
5. References	23
5.1 Documents	23
5.2 Appendix A: Definitions.....	23
5.3 Appendix B: Example PIA and Collaboration Agreement.....	23

1. Introduction

1.1 Purpose

This document presents requirements for controlling the exchange of data, information and intellectual property. The requirements are defined in the context of the Information Labeling & Handling (ILH) project, but are applicable to any collaborative scenario that involves exchange of data, information and intellectual property.

1.2 Overview of Intellectual Property

Intellectual Property (IP) is the manifestation of an individual's intellectual creativity. If the owners of such IP take certain steps, for example, by registering the mental creation with national agencies, they are afforded the opportunity to exploit certain monopoly rights for monetary gain. Equally, some IP rights automatically subsist on their creation. IP owners may profit from their IP directly through the sale of products or indirectly through licensing. In the United States, the main categories of IP are: copyright, trademarks, patents, design rights and trade secrets. All these categories of IP are recognized internationally, but the terms of application, registration and protection vary from country to country.

2. Intellectual Property Business Scenarios

The TSCP Intellectual Property Working Group (IPWG) has identified the following business scenarios for obtaining and implementing the exchange of information and IP between two or more organizations under a number of different contractual mechanisms, and determining whether access to the information or IP can be provided to a given user.

The business scenarios in this paper do not reflect any specific Agreement, but are examples of a few scenarios that could be supported by technologies such as the ones proposed for the TSCP ILH project. Current practices vary widely among participants and are often based on manual processes. The IPWG hopes that implementation of TSCP capabilities supporting the business scenarios will simplify the process of managing IP Agreements and ensuring compliance, while reducing the risk of non-compliance and information leakage, as well as reducing the overall cost of compliance through development, implementation and adoption of appropriate industry standards.

In particular, the business scenarios presented here classify activities that may be *assisted* by electronic systems (shown as blue boxes in the process flow diagrams), *fully automated* (shown as green boxes in the process flow diagrams), as well as *optional flows* (indicated by dotted lines). Although these systems do not exist today, this paper intends to highlight the business activities that may benefit from such automation if the proper procedures and appropriate security controls are implemented.

The business scenarios presented in this paper are:

1. Proprietary Information Agreements (PIA)
2. Collaborative Agreements
3. Sub-Tier Supplier Agreements

2.1 Business Scenario 1: Proprietary Information Agreement (PIA) Implementation Process

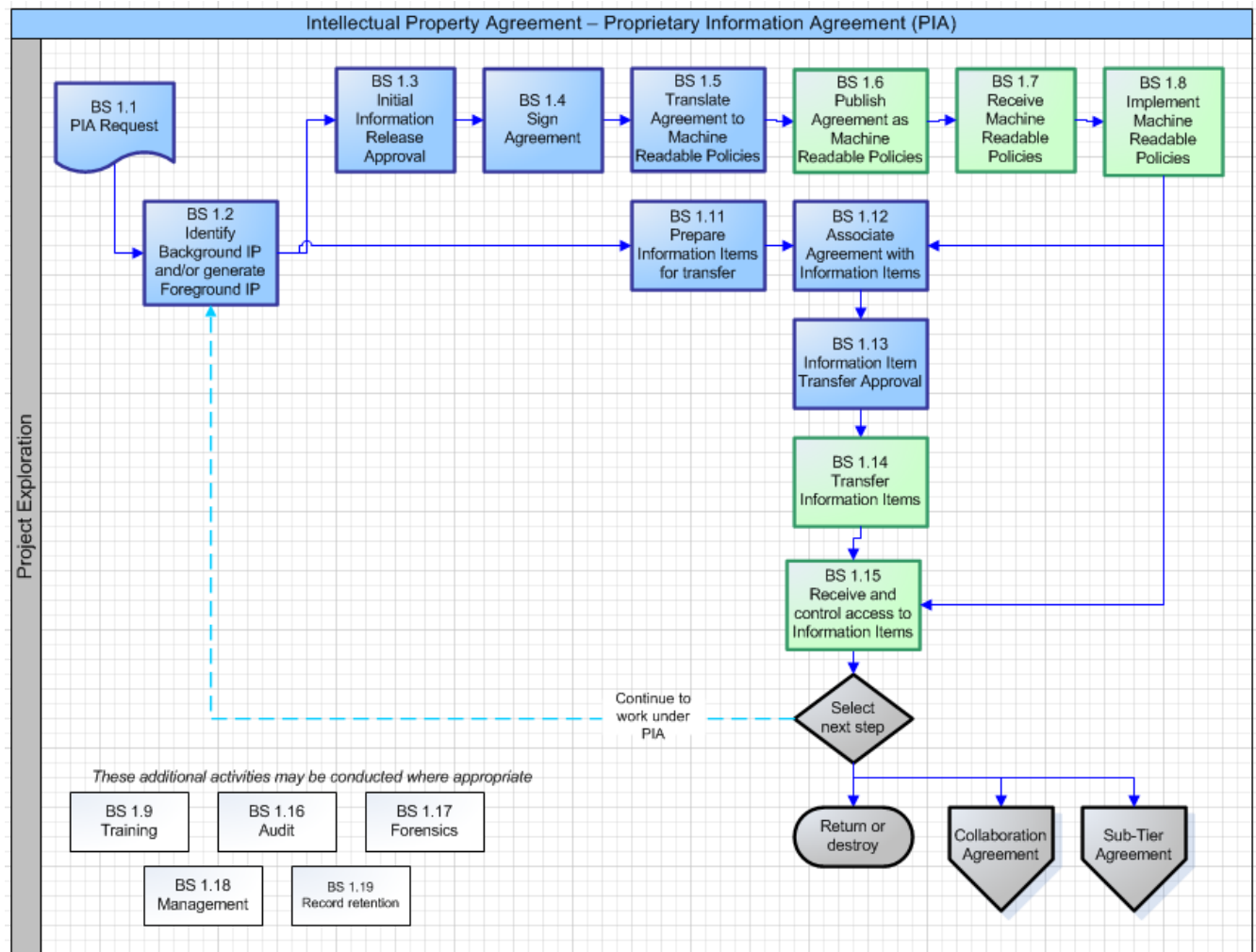
When organizations need to explore possible collaborative projects, they first create and sign “Proprietary Information Agreements”, or PIAs. These documents describe the nature of the possible collaboration, identify information to be exchanged, and require all parties to the PIA to agree to protect the information under the terms of the agreement. The process flow, discrete steps and detailed descriptions follow.

The following entities are defined for the first set of IP use cases. The terms “Disclosing party” and “Receiving party” are used in accordance with standard contractual practice.

Entity Descriptions:

Entity Name	Description
Disclosing party	An entity providing access to controlled information, and will sign a PIA to support collaboration.
Receiving party	An entity with a need for access to controlled information who will sign a PIA to support collaboration
Agreement (PIA)	Proprietary Information Agreement (PIA) - the legal document, or contract, that allows exchange of information between two or more organizations according to specific terms.

Background IP is created before the Agreement while Foreground IP is created under the Agreement.



Legend:

- BLUE BOXES** = Assisted
- GREEN BOXES** = Fully Automated
- DOTTED LINES** = Optional flows (may not occur in every instance)

PIA Implementation Process Steps

The first step in exploration of a collaborative program is implementation of a PIA, which includes the following steps:

Scenario #	Process Step	Participant(s)	Description
BS 1.1	PIA request	Disclosing party and Receiving party(ies)	The program manager collects a list of partners with whom information must be shared.
BS 1.2	Identify Background IP and/or generate Foreground IP	Disclosing party and Receiving party(ies)	Information to be shared under the Agreement must be identified or created. There can be requests from the Receiving Party as well as suggestions by the Disclosing Party.
BS 1.3¹	Initial Information Release Approval	Disclosing party	The Disclosing party information owners determine the scope of information objects that are approved for sharing. At this stage this may involve specific items or general classes of information.
BS 1.4	Sign Agreement	Disclosing party and Receiving party(ies)	Authorized representatives from Disclosing party and Receiving party agree upon terms and sign the Agreement.
BS 1.5²	Translate Agreement to Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Agreement is translated into a computer readable format that can be directly interpreted by electronic systems or translated into an appropriate access control implementation (e.g. XACML.)
BS 1.6	Publish Agreement as Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Machine Readable Policies are provided to those organizations that will be handling the Information Items.
BS 1.7	Receive Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items receive the Machine Readable Policies.
BS 1.8	Implement Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items implement the Machine Readable Policies into the labeling, identity and access control systems. The systems will be tested to ensure that the Information Items can be protected as required by the Agreement. Each Receiving party will implement appropriate access

¹ **Applies to all X.3 references in this document: Additional Release Approval:** If additional information objects, not identified as in-scope during the Initial Information Release Approval process, are to be shared with receiving parties, then a further iteration of the Information Release Approval process is engaged to amend or extend the Agreement to cover the additional information. In-scope information items may continue to be released as necessary subject to Information Item Transfer Approval.

² **Applies to all X.5 references in this document: Translate Agreement to Machine Readable Format:** This process step includes the Disclosing party analyzing and adjudicating the agreement for conflicts with other contracts. A conflict is defined as a condition in which the restrictions on the exchange of information defined in one Agreement may not be enforced because that would breach the terms of another Agreement. If any conflicts exist, a resolution must be determined. A strategic goal is to have the adjudication process take place programmatically in software.

Scenario #	Process Step	Participant(s)	Description
			controls within their systems by associating the machine readable policies with the information exchanged under the Agreement.
BS 1.9	Training	Disclosing party and Receiving Parties	The participants will develop training materials for program participants which will address identification of sensitive material, knowledge of the Agreement and knowledge of labeling and sharing guidelines for the program. If necessary, the participants will supplement developed training material with local requirements/guidelines. Management at each program participant will deliver training to their team. The participants may use training provided by other participants or may create their own training, as required by policy.
BS 1.10	N/A	N/A	N/A
BS 1.11	Prepare Information Items for transfer	Disclosing party	The content of the Information Items is prepared and approved, as necessary, through appropriate functional and program procedures.
BS 1.12	Associate Agreement with Information Items	Disclosing party	Apply appropriate metadata tags and markings to Information Items to be shared
BS 1.13	Information Item Transfer Approval	Disclosing party	Execute any release process for the individual Information Items. In some cases this may be a decision of the information worker and in others there may be a need for independent specialist or management approval.
BS 1.14	Transfer Information Items	Disclosing party	Disclosing party transfers or provides access to the Information Items using tools such as TSCP Secure Email or a collaborative environment.
BS 1.15	Receive and control access to Information Items	Receiving Party and their designated agents	The Receiving Party and any agents providing systems control access to locally held copies of the Information Items. The Disclosing Party may continue to control access to Information Items held in collaborative environments.
BS 1.16	Audit	Disclosing party, Receiving Parties and their designated agents	All parties verify that systems comply with the Agreement by jointly defining audit collection and reporting guidelines. Relevant personnel working for organizations affiliated with the program will perform periodic audits of systems and access records to confirm that controls have been implemented correctly and are effectively protecting program information.

Scenario #	Process Step	Participant(s)	Description
BS 1.17	Forensics	Disclosing party, Receiving Parties and their designated agents	All parties will make provisions for forensic analysis in the case of suspected breaches or information leaks.
BS 1.18	Management	Disclosing party, Receiving Parties and their designated agents	Relevant personnel working for organizations affiliated with the program will ensure that systems access control is maintained and monitored appropriately, with a periodic review of users and entitlements.
BS 1.19	Record Retention	Disclosing party, Receiving Parties and their designated agents	All parties will retain and make available if required records regarding transactions under the Agreement. Information Items will be destroyed or returned by the Receiving Party as required under the Agreement at expiry or termination.

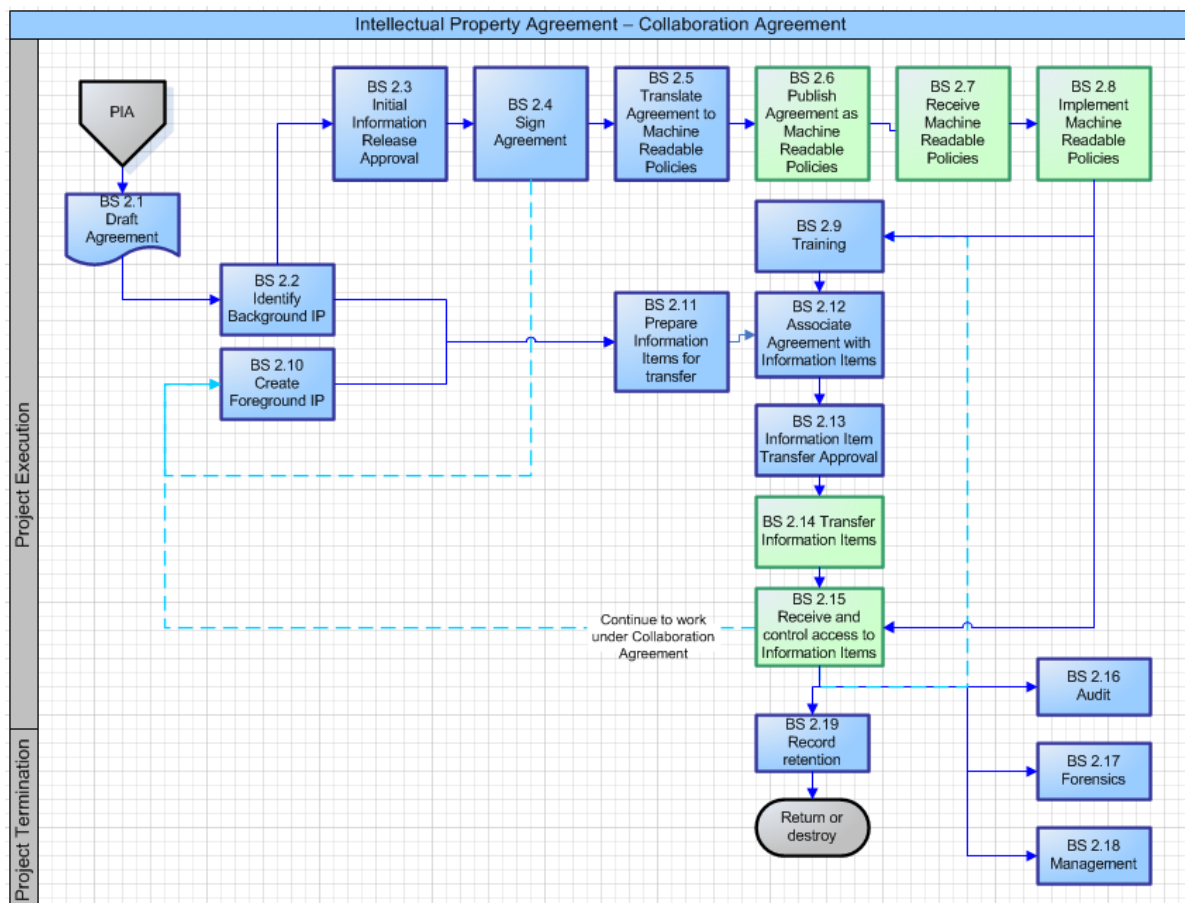
2.2 Business Scenario 2: Collaborative Agreements

If, during the course of the project exploration phase, parties to the PIA decide to proceed with a formal collaboration project, the next step is for all parties to create and sign collaborative agreements. The collaborative agreement is generally more comprehensive than a PIA, as rights to background and foreground IP are well-defined; thorough lists of information to be exchanged are attached as schedules or appendices; and contractual obligations specify exactly how information is to be protected and dispositioned. The process flow, discrete steps and detailed descriptions follow.

Entity Descriptions

The following entities have been defined for Business Scenarios 2.2

Entity Name	Description
Receiving Party	Licensee - An entity with a need for access to controlled information or IP to support the collaboration
Disclosing Party	Licensor - The owner of the IP or information and providing access to the controlled information or IP to support the collaboration.
Agreement	Collaboration Agreement - A legal document or contract that allows exchange of information or IP between two or more organizations according to specific terms to support a collaboration arrangement.



Legend:

- BLUE BOXES** = Assisted
- GREEN BOXES** = Fully Automated
- DOTTED LINES** = Optional flows (may not occur in every instance)

Collaborative Agreements Process Steps

Scenario #	Process Step	Participant(s)	Description
BS 2.1	Draft Agreement	Disclosing party and Receiving party(ies)	The parties create tailored collaboration Agreement for the program based on pro forma.
BS 2.2	Identify Background IP	Disclosing party and Receiving party(ies)	Information to be shared under the Agreement must be identified or created. There may be requests from the Receiving Party as well as suggestions by the Disclosing Party.
BS 2.3	Initial Information Release Approval	Disclosing party	The Disclosing party information owners determine the scope of information objects that are approved for sharing. At this stage this may involve specific items or general classes of information.
BS 2.4	Sign Agreement	Disclosing party and Receiving party(ies)	Authorized representatives from Disclosing party and Receiving party agree upon terms and sign the Agreement.
BS 2.5	Translate Agreement to Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Agreement is translated into a computer readable format that can be directly interpreted by electronic systems or translated into an appropriate access control implementation (e.g. XACML.)
BS 2.6	Publish Agreement as Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Machine Readable Policies are provided to those organizations that will be handling the Information Items.
BS 2.7	Receive Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items receive the Machine Readable Policies.
BS 2.8	Implement Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items implement the Machine Readable Policies into the labeling, identity and access control systems. The systems will be tested to ensure that the Information Items can be protected as required by the Agreement. Each Receiving party will implement appropriate access controls within their systems by associating the machine readable policies with the information exchanged under the Agreement. If the Disclosing Party hosts Information Items in its own collaboration environment, the policies translated into machine readable format will be implemented into electronic access control policies for the target collaboration systems.
BS 2.9	Training	Disclosing party and Receiving Parties	The participants will develop training materials for program participants that address identification of sensitive material, knowledge of the Agreement and knowledge of labeling and sharing guidelines for the program. If necessary, the participants will supplement developed

Scenario #	Process Step	Participant(s)	Description
			training material with local requirements/guidelines. Management at each program participant will deliver training to their team. The participants may use training provided by other participants or may create their own training, as required by policy.
BS 2.10	Create Foreground IP	Disclosing party	Under the terms of the Agreement and party may create creating new IP. The new IP ownership is governed by the Agreement, and newly created information is prepared in an ongoing fashion. This foreground IP can then be disclosed to other parties in accordance with the Agreement.
BS 2.11	Prepare Information Items for transfer	Disclosing party	The content of the Information Items is prepared and approved, as necessary, through appropriate functional and program procedures.
BS 2.12	Associate Agreement with Information Items	Disclosing party	Apply appropriate metadata tags and markings to Information Items to be shared
BS 2.13	Information Item Transfer Approval	Disclosing party	Execute any release process for the individual Information Items. In some cases this may be a decision of the information worker and in others there may be a need for independent specialist or management approval.
BS 2.14	Transfer Information Items	Disclosing party	Disclosing party transfers or provides access to the Information Items using tools such as TSCP Secure Email or a collaborative environment.
BS 2.15	Receive and control access to Information Items	Receiving Party and their designated agents	The Receiving Party and any agents providing systems control access to locally held copies of the Information Items. The Disclosing Party may continue to control access to Information Items held in collaborative environments.
BS 2.16	Audit	Disclosing party, Receiving Parties and their designated agents	All parties verify that systems comply with the Agreement by jointly defining audit collection and reporting guidelines. Relevant personnel working for organizations affiliated with the program will perform periodic audits of systems and access records to confirm that controls have been correctly implemented and are effectively protecting program information.
BS 2.17	Forensics	Disclosing party, Receiving Parties and their designated agents	All parties will make provisions for forensic analysis in the case of suspected breaches or information leaks.

Scenario #	Process Step	Participant(s)	Description
BS 2.18	Management	Disclosing party, Receiving Parties and their designated agents	Relevant personnel working for organizations affiliated with the program will ensure that systems access control is maintained and monitored appropriately, with a periodic review of users and entitlements.
BS 2.19	Record Retention	Disclosing party, Receiving Parties and their designated agents	All parties will retain and make available, if required, records regarding transactions under the Agreement. Information Items will be destroyed or returned by the Receiving Party as required under the Agreement at expiry or termination.

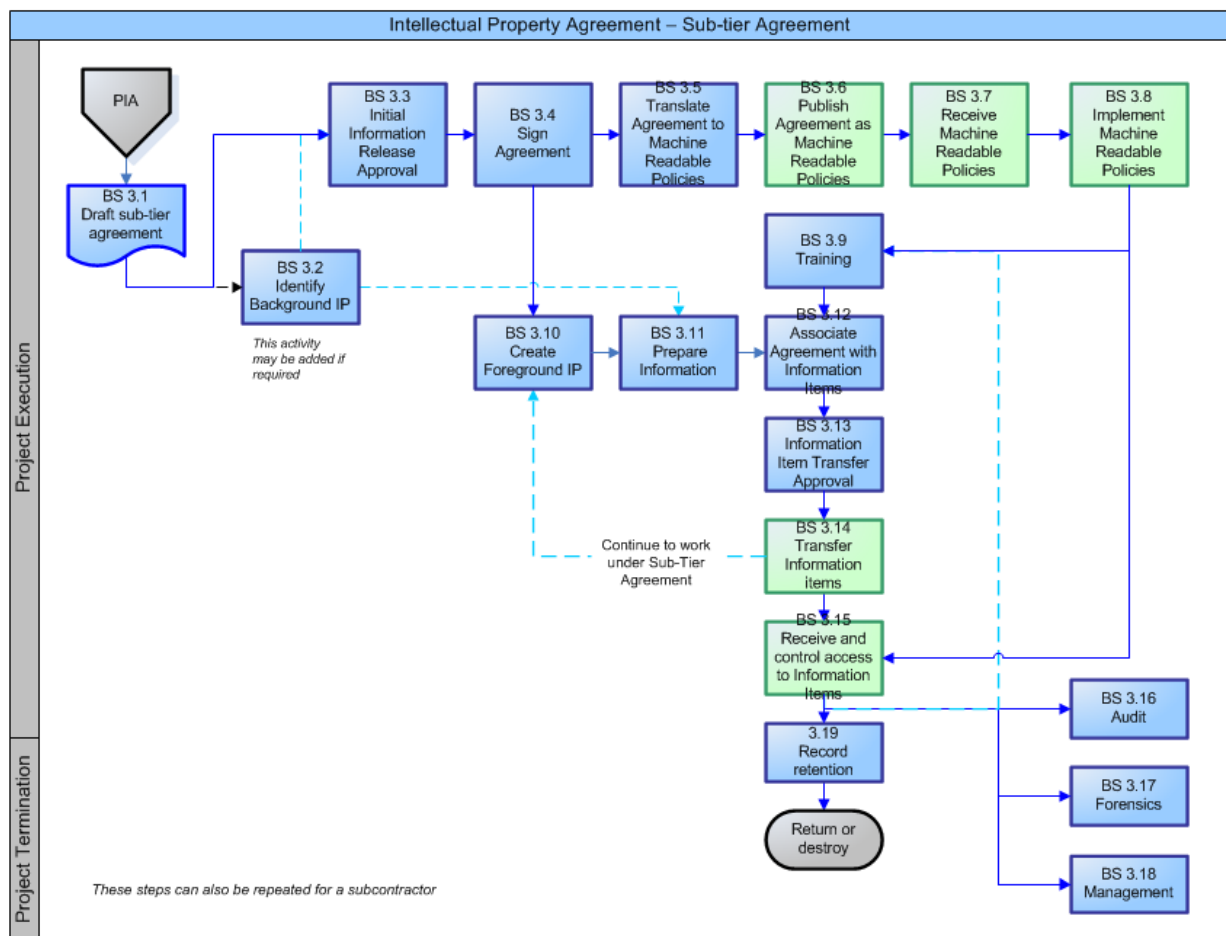
2.3 Business Scenario 3: Sub-Tier Supplier Agreements

If, during the course of the collaboration, parties to the collaboration agreement decide to engage subcontractors, the next step is for all parties to create and sign sub-tier supplier agreements. The sub-tier supplier agreement is generally tailored to the specific legal relationship between the primary contractor and subcontractors, as rights to background and foreground IP are well-defined; thorough lists of information to be exchanged are attached as schedule or appendices; and contractual obligations specify exactly how information is to be protected and dispositional. The process flow, discrete steps and detailed descriptions follow.

Entity Descriptions

The following entities have been defined for Business Scenarios 2.3

Entity Name	Description
Receiving Party	Licensee - An entity with a need for access to controlled information or IP to support the collaboration
Disclosing Party	Licensor - The owner of the IP or information and providing access to the controlled information or IP to support the collaboration.
Agreement	Collaboration Agreement - A legal document or contract that allows exchange of information or IP between two or more organizations according to specific terms to support a collaboration arrangement.



Legend:

- BLUE BOXES** = Assisted
GREEN BOXES = Fully Automated
DOTTED LINES = Optional flows (may not occur in every instance)

Sub-Tier Supplier Agreement Process Steps

Scenario #	Process Step	Participant(s)	Description
BS 3.1	Draft Sub-Tier Agreement	Disclosing party and Receiving party(ies)	The parties create tailored Sub-Tier Agreement for the program based on pro forma.
BS 3.2	Identify Background IP	Disclosing party and Receiving party(ies)	Information to be shared under the Agreement must be identified or created. There may be requests from the Receiving Party as well as suggestions by the Disclosing Party.
BS 3.3	Initial Information Release Approval	Disclosing party	The Disclosing party information owners determine the scope of information objects that are approved for sharing. At this stage this may involve specific items or general classes of information.
BS 3.4	Sign Agreement	Disclosing party and Receiving party(ies)	Authorized representatives from Disclosing party and Receiving party agree upon terms and sign the Agreement.
BS 3.5	Translate Agreement to Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Agreement is translated into a computer readable format that can be directly interpreted by electronic systems or translated into an appropriate access control implementation (e.g. XACML.)
BS 3.6	Publish Agreement as Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The Machine Readable Policies are provided to those organizations that will be handling the Information Items.
BS 3.7	Receive Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items receive the Machine Readable Policies.
BS 3.8	Implement Machine Readable Policies	Disclosing party or Receiving party(ies) or their designated agents	The organizations that will be handling the Information Items implement the Machine Readable Policies into the labeling, identity and access control systems. The systems will be tested to ensure that the Information Items can be protected as required by the Agreement. Each Receiving party will implement appropriate access controls within their systems by associating the machine readable policies with the information exchanged under the Agreement. If the Disclosing Party hosts Information Items in its own collaboration environment, the policies translated into machine readable format will be implemented into electronic access control policies for the target collaboration systems.
BS 3.9	Training	Disclosing party and Receiving Parties	The participants will develop training materials for program participants that address identification of sensitive material, knowledge of the Agreement and knowledge of labeling and sharing guidelines for the program. If necessary,

Scenario #	Process Step	Participant(s)	Description
			the participants will supplement developed training material with local requirements/guidelines. Management at each program participant will deliver training to their team. The participants may use training provided by other participants or may create their own training, as required by policy.
BS 3.10	Create Foreground IP	Disclosing party	Under the terms of the Agreement and party may create new IP. The new IP ownership is governed by the Agreement, and newly created information is prepared in an ongoing fashion. This foreground IP can then be disclosed to other parties in accordance with the Agreement.
BS 3.11	Prepare Information Items for transfer	Disclosing party	The content of the Information Items is prepared and approved, as necessary, through appropriate functional and program procedures.
BS 3.12	Associate Agreement with Information Items	Disclosing party	Apply appropriate metadata tags and markings to Information Items to be shared
BS 3.13	Information Item Transfer Approval	Disclosing party	Execute any release process for the individual Information Items. In some cases this may be a decision of the information worker and in others there may be a need for independent specialist or management approval.
BS 3.14	Transfer Information Items	Disclosing party	Disclosing party transfers or provides access to the Information Items using tools such as TSCP Secure Email or a collaborative environment.
BS 3.15	Receive and control access to Information Items	Receiving party and their designated agents	The Receiving party and any agents providing systems control access to locally held copies of the Information Items. The Disclosing party may continue to control access to Information Items held in collaborative environments.
BS 3.16	Audit	Disclosing party, Receiving Parties and their designated agents	All parties verify that systems comply with the Agreement by jointly defining audit collection and reporting guidelines. Relevant personnel working for organizations affiliated with the program will perform periodic audits of systems and access records to confirm that controls have been correctly implemented and are effectively protecting program information.
BS 3.17	Forensics	Disclosing party, Receiving parties and their designated agents	All parties will make provisions for forensic analysis in the case of suspected breaches or information leaks.
BS 3.18	Management	Disclosing party, Receiving parties and	Relevant personnel working for organizations affiliated with the program

Scenario #	Process Step	Participant(s)	Description
		their designated agents	will ensure that systems access control is maintained and monitored appropriately, with a periodic review of users and entitlements.
BS 3.19	Record Retention	Disclosing party, Receiving parties and their designated agents	All parties will retain and make available if required records regarding transactions under the Agreement. Information Items will be destroyed or returned by the Receiving party as required under the Agreement at expiry or termination.

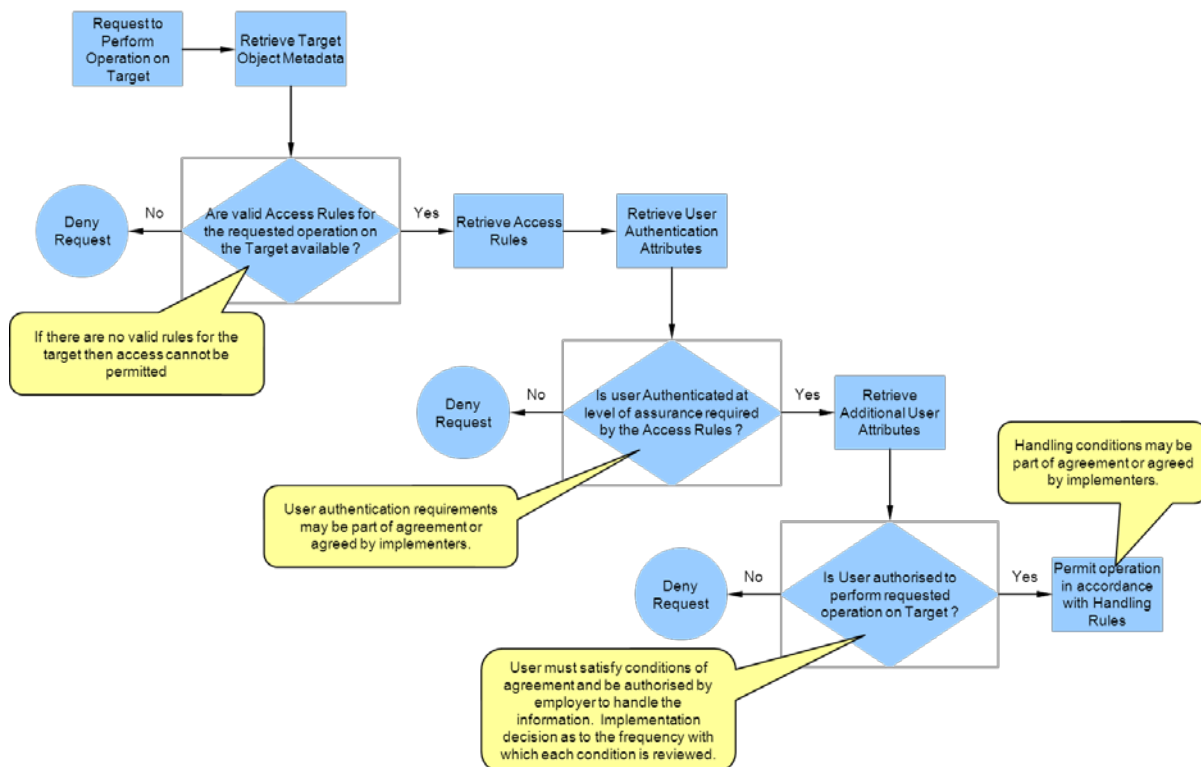
*These steps may also be repeated for a subcontractor.

3. IP Access Authorization Flow

The IP Working Group has developed a process flow describing the steps required to determine whether an information or IP object may be shared with a given requestor. These steps are the basic information and IP release logic that moves you from 3.4 to 3.7 of technical release process to verify that the release is authorized.

The process flow identifies the following participants:

Entity Name	Description
Authorized User (End User)	An individual requesting access to a controlled information or IP object. Actions or decisions present in this functional row reflect determination of attributes regarding the user themselves.
Information or IP Object	Actions or decisions in this function row represent the determination of the protection requirements governing the information or IP object.
Business Agreement	This entity represents an Agreement to share information or license IP. This functional row presents determinations regarding the existence of an authority to such information or IP.
Licensor	The owner of the IP or information. This functional row presents tasks for which the Licensor is responsible.



These processes make the following assumptions about the environment in which the request is being made:³

- The user has been authenticated, and all Agreement attributes required to make access control decisions⁴ are available to systems protecting controlled data.
- Information and IP Objects have been appropriately labeled to indicate their status as controlled information or IP, and correspond with Business Agreements that grant access to the information or IP.
- The Business Agreements governing access to the technical information have been approved by the relevant policy authorities, and electronic systems protecting the information can interpret the Business Agreements directly and determine whether a document can be released, given the required information about users and information or IP objects.

³ See http://pubs.opengroup.org/onlinepubs/009609199/chap3.htm#tagfcjh_1 for an example of an access control decision/enforcement flow.

4. Requirements

4.1 Process Steps - Requirements

BS*.1	Draft Agreement
Participants	Licensor and licensee
Description	Licensor creates a tailored Agreement for program or object based on pro forma.
Outputs	Drafted Agreement
Requirements	Terms and conditions must adequately cover scope and protection requirements of material to be shared for the duration of the Agreement.
Notes	

BS*.2	Identify Background IP
Participants	Disclosing party or Licensor
Description	Parties identify background IP to be shared with partners
Outputs	Content to be shared is identified as an exhibit attached to the Agreement
Requirements	All information to be shared under the Agreement is identified
Notes	For PIA Agreements this is described as covering foreground too, see BS *.9

BS*.3	Initial Release Approval Process
Participants	Licensor or Disclosing Party
Description	The Licensor's information owners determine which information objects may be shared and with which potential Licensees.
Outputs	Approval
Requirements	Must conform to internal release policies
Notes	

BS*.4	Sign Agreement
Participants	Licensor and Licensee(s) or Disclosing Parties
Description	Authorized representatives from Licensor and Licensee will agree upon terms and sign the Agreement.
Outputs	Signed Agreement
Requirements	Must conform to internal release policies
Notes	Only authorized representatives and/or individuals who have been legally and/or appropriately delegated with signing authority may sign the Agreement

BS*.5	Translate Agreement into Computer Readable format
Participants	Licensor or Disclosing Parties
Description	Following approval of the Agreement required by the program, the Agreement is translated into a computer readable format that can be directly interpreted by electronic systems or translated into an appropriate access control implementation

BS*.5 Translate Agreement into Computer Readable format	
	(e.g. XACML).
Outputs	XACML access control policies
Requirements	Must adhere to TSCP ILH BAILS
Notes	This process step includes the Licensor analyzing and adjudicating the Agreement for conflicts with other contracts. A conflict is defined as a condition where the restrictions on the exchange of information defined in one Agreement cannot be made because it would breach the terms of another Agreement. If any conflicts exist, a determination is made of the best way to resolve the conflict. A strategic goal is to have the adjudication process take place programmatically in software.

BS*.6 Publish Agreement as Machine Readable Policies	
Participants	Licensor and/or Licensees
Outputs	Machine Readable Policy
Requirements	Must be in a format that partners can utilize
Notes	The Machine Readable Policies are provided to those organizations that will be handling the Information Items

BS*.7 Receive Machine Readable Policies	
Participants	Licensor and/or Licensees
Outputs	Machine Readable Policies
Requirements	Must be translated into required internal formats
Notes	The organizations that will be handling the Information Items receive the Machine Readable Policies.

BS*.8 Implement Machine Readable Policies	
Participants	Licensor and/or Licensees
Outputs	Systems that are configured to operate in accordance with the Machine Readable Policies
Requirements	Must be tested with partners.
Notes	The organizations that will be handling the Information Items implement the Machine Readable Policies into the labeling, identity and access control systems. The systems will be tested to ensure that the Information Items can be protected as required by the Agreement. Each Receiving party will implement appropriate access controls within their systems by associating the machine readable policies with the information exchanged under the Agreement. If the Disclosing Party hosts Information Items in its own collaboration environment, the policies translated into machine readable format will be implemented into electronic access control policies for the target collaboration systems.

BS*.9	Training
Participants	Licensor and/or Licensees
Description	The participants will develop training materials for program participants that addresses identification of sensitive material, knowledge of the Agreement and knowledge of labeling and sharing guidelines for the program. If necessary, the participants will supplement developed training material with local requirements/guidelines. Management at each program participant will deliver training to their team. External entities may use training provided by the Licensor, or may create their own training as required by policy.
Outputs	Training materials, confirmation of training
Requirements	Training must conform to appropriate laws, regulations, and internal policies of parties to the Agreement
Notes	Training may be web-based, and may be delivered by Licensor

BS*.10	Create Foreground IP
Participants	Licensor and Licensees
Description	Under the terms of the Agreement, both Licensor and Licensees work together creating new IP. The new IP ownership is governed by the Agreement, and newly created information is prepared in an ongoing manner as in step BS*.6.
Outputs	Foreground IP objects
Requirements	Properly tagged with accurate metadata
Notes	Licensor and Licensees

BS*.11	Prepare Information Items for Transfer
Participants	Licensor or Disclosing Party
Description	Licensor (and Licensee, if needed) apply appropriate metadata tags, labels, and encryption to information to be shared.
Outputs	Information objects to be shared are properly tagged with accurate metadata
Requirements	Files encrypted for transmission
Notes	Parties must agree on which encryption type they will use for the exchange

BS*.12	Associate Agreement with Information Items
Participants	Licensor and/or Licensees
Outputs	Information Items that are marked and contain metadata
Requirements	Meta-data must enable the application of policy Meta-data must be in a format that recipients can utilize
Notes	Apply appropriate metadata tags and markings to Information Items to be shared

BS*.13	Information Item Transfer Approval
Participants	Licensor or Disclosing Party
Description	If additional information objects, not identified during initial release approval process, are to be shared with Licensees, then a secondary release approval process is engaged.
Outputs	Approval
Requirements	Must conform to internal release policies
Notes	

BS*.14	Transfer Information Items
Participants	Licensors, Licensees and/or their designated agents
Description	Licensor will provide IP or access to Information using TSCP Secure Email or a collaborative environment. The systems will be tested to ensure that the information and IP objects can be protected as required by the Agreement. Each participant implements access controls in relevant systems to ensure that controlled assets are adequately protected based on conditions defined within the Agreement or relevant policy documents.
Outputs	Marked, meta-data tagged and possibly encrypted files
Requirements	Licensees and/or their designated agents must have access control systems that conform to the XACML language/protocol
Notes	In cases where Licensor hosts IP in its own collaboration environment, the policies translated into machine readable format will be implemented into electronic access control policies for the target collaboration systems. In cases where the Licensor transmits IP to Licensees, the Licensee will take the translated access control policies and implement them into their target collaboration systems.

BS*.15	Receive and control access to information items
Participants	Licensor and/or Licensees
Outputs	Controlled access to Information Items
Requirements	Authentication and authorization information must be provided to the System Operator in a consistent manner Information Items are marked and meta-data tagged in a consistent manner.
Notes	The Receiving party and any agents providing systems control access to locally held copies of the Information Items. The Disclosing party may continue to control access to Information Items held in collaborative environments.

BS*.16	Audit
Participants	Licensor and Licensee
Description	The Licensor will verify that systems comply with the Agreement by jointly defining audit collection and reporting guidelines. Relevant personnel working for organizations affiliated with the program will perform periodic audits of systems and access records to confirm that controls have been correctly implemented and are effectively protecting program information and IP.

BS*.16	Audit
Outputs	Audit reports
Requirements	Audit terms and conditions shall be listed in the Agreement
Notes	

BS*.17	Forensics
Participants	Licensor and Licensee
Description	Licensee will make provisions for Licensor to conduct forensic analysis in the case of suspected breaches or information leaks.
Outputs	Forensic investigation case details
Requirements	Details on how Licensor may require or conduct forensic investigations with Licensees should be addressed in the Agreement.
Notes	

BS*.18	Management
Participants	Licensor and Licensee
Description	Relevant personnel working for organizations affiliated with the work effort will ensure that systems access control is maintained and monitored appropriately, with a periodic review of users and permissions.
Outputs	Accurate and current user information, including appropriate permissions for accessing licensed information.
Requirements	Details on user information currency should be addressed in the Agreement
Notes	

BS*.19	Record Retention
Participants	Licensor and Licensee
Description	Licensee will retain and make available to Licensor records regarding transactions involving Licensor IP, as specified in the Agreement.
Outputs	Information access transaction logs
Requirements	Details on record retention should be addressed in the Agreement
Notes	Logs may be in standard syslog format

5. References

5.1 Documents

TSCP Information Labeling and Handling

The following reference documents may be found at <http://www.tscp.org/ilh/>:

Business Authorization Framework Version 1 BAF v.1

Business Authorization Identification and Labeling Scheme Version 1 (BAILS v.1.0)

5.2 Appendix A: Definitions

Collaborative Agreement: For the purpose of this document, this term is used to describe entities involved in collaborative or teaming arrangement in which information is exchanged and IP licensed in the performance of work. Entities may assume any of the following roles:

Primary Contractor: An entity who holds the master contract with a customer.

Supplier: An entity who supplies technical data and products for a collaborative effort, with the intent of sharing technical data with collaborators.

Sub-Contractor: An entity who receives a license from a Supplier in support of a build-to-print contract.

Licensor: An entity who grants rights for the usage of its IP.

Licensee: An entity who receives a license to use IP.

PIA: A Proprietary Information Agreement sometime referred to as a non-disclosure Agreement (NDA).

5.3 Appendix B: Example PIA and Collaboration Agreement

Curtiss Packard PIA Example:

<https://tscp.sharesrvr.com/IPWG/508%20Intellectual%20Property%20Working%20Group/508.02%20Requirements/IPWG%20Curtis%20Packard%20PIA.doc>

<https://tscp.sharesrvr.com/IPWG/508%20Intellectual%20Property%20Working%20Group/508.02%20Requirements/ZD1267%20Curtiss-Spad%20PIA%20TSCP.doc>

Collaboration Agreement Example:

<https://tscp.sharesrvr.com/IPWG/508%20Intellectual%20Property%20Working%20Group/508.02%20Requirements/Collaboration%20Agreement%20Sample%20TSCP.docx>