For the results of the survey, please see:
https://www.surveymonkey.com/results/SM-BJRDWBB97/

Based on the survey results, EPDP Leadership proposes the following order for upcoming calls:

EPDP Team Meeting	Topics
1 August 2019	**Group 2 - First reading continued**: Investigation of criminal activity where domain names are used. Typical specific example: phishing attack (SSAC 3) **Group 4** - **First reading**: Online buyers identifying and validating the source or services/ Internet users validating the legitimacy of an email or a website to protect themselves (ALAC 1) *(Note that SSAC2 scored marginally higher, but due to unavailability of SSAC reps for this meeting, the leadership team decided to commence with this use case)*
2 August 2019	Member to submit edit/view/proposals for SSAC 3 and ALAC 1 in writing
6 August 2019	Use case authors, with staff support as needed, to distribute updated SSAC 3 and ALAC 1 use cases, incorporating input received
8 August 2019	**Group 2 – Second/final reading**: Investigation of criminal activity where domain names are used. Typical specific example: phishing attack (SSAC 3) **Group 4 - First reading continued**: Online buyers identifying and validating the source or services/ Internet users validating the legitimacy of an email or a website to protect themselves (ALAC 1)
9 August 2019	Member to submit edit/view/proposals for ALAC 1 in writing
13 August 2019	Use case author, with staff support as needed, to distribute updated ALAC 1 use case, incorporating input received. Final version of SSAC 3 use case to be distributed by use case author, with staff support as needed, and posted on wiki.
15 August 2019	**Group 5 – First reading:** Providers requesting access required to facilitate due process in the UDRP and URS (IP 5) *(Note, this use case was tied with BC6 but as this use case was also discussed during phase 1, the leadership team recommends starting with this one)* **Group 2 – Second/final reading**: Online buyers identifying and validating the source or services/ Internet users validating the legitimacy of an email or a website to protect themselves (ALAC 1)
16 August 2019	Member to submit edit/view/proposals for IP 5 in writing
13 August 2019	Use case author, with staff support as needed, to distribute updated IP 5 use case, incorporating input received. Final version of ALAC 1 use case to be distributed by use case author, with staff support as needed, and posted on wiki.

15 August 2019	**Group 3 - First reading**: When a network is undergoing an attack involving a domain name, and the operator(s) of that network need to contact the domain owner to remediate the security issue (DDOS, Botnet, etc.) (SSAC1) **Group 5 – Second/final reading**: Providers requesting access required to facilitate due process in the UDRP and URS (IP 5)
16 August 2019	Member to submit edit/view/proposals for SSAC 1 in writing
16 August 2019	EPDP Team to identify which use cases, or aspects of use cases, in each category are significantly different from use case already reviewed and need to be considered further.
20 August 2019	Use case author, with staff support as needed, to distribute updated SSAC 1 use case, incorporating input received. Final version of IP 5 use case to be distributed by use case author, with staff support as needed, and posted on wiki.
22 August 2019	**Group 3 – Second/final reading**: When a network is undergoing an attack involving a domain name, and the operator(s) of that network need to contact the domain owner to remediate the security issue (DDOS, Botnet, etc.) (SSAC1) **Group 1 – first reading, second use case** (to be determined based on input received by 16 August)
23 August 2019	
29 August 2019	**Group 1 – second/final reading, second use case** **Group 2 – first reading, second use case** (to be determined based on input received)
End August / Early September	**Leadership team to share draft policy principles / recommendations derived from use case review for review and discussion during F2F meeting, incl. proposed schedule to continue review of use cases, if deemed necessary.**

Use Case Categorization

Group 1: Criminal Law enforcement/national or public security	LEA 1, LEA 2, IP 2, IP 3
Group 2: Non-LE investigations and civil claims	BC1/2, BC 3, BC 5, SSAC 3, ALAC 2, IP 1, IP 4
Group 3: Need for redacted data for a third party to contact registrant	BC 7, SSAC 1
Group 4: Consumer protection, abuse prevention, digital service provider (DSP) and network security	SSAC 2, BC 9, ALAC 1
Group 5: Registered Name Holder consent or contract	BC 4, BC 6, BC 8, IP 5

LEGEND

LEA 1	Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a non-local data controller.
LEA 2	Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a local data controller.
SSAC 1	When a network is undergoing an attack involving a domain name, and the operator(s) of that network need to contact the domain owner to remediate the security issue (DDOS, Botnet, etc.)
SSAC 2	Determine "Reputation" of domain name and/or elements associated with domain name registrations.
SSAC 3	Investigation of criminal activity where domain names are used. Typical specific example: phishing attack.
IP 1	Trademark owners requesting data in the establishment, exercise or defense of legal claims for trademark infringement
IP 2	Investigation of criminal activity against a victim in the jurisdiction of the investigating LEA requesting data from either a local a non-local data controller. (criminal trademark)
IP 3	Investigation of criminal activity in the jurisdiction of the investigating LEA requesting data from either a local a non-local data controller. (criminal copyright)
IP 4	Copyright owners requesting data in the establishment, exercise or defense of legal claims for copyright infringement
IP 5	Providers requesting access required to facilitate due process in the UDRP and URS
BC1/2	Initial investigation of criminal activity against a victim and/or secondary victim where domain names are used in the commission of the crime
BC 3	Identify owner of abusive domains and other related domains involved in civil legal claims related to phishing, malware, botnets, and other fraudulent activities
BC 4	Maintaining the domain name registration by the Registered Name Holder
BC 5	The establishment, exercise or defense of a legal claim involving a registrant of a domain name
BC 6	M&A name portfolio due diligence or purchase of domain name from bankrupt entity or other seller
BC 7	Contacting the Registrant to resolve a Technical or Operational Issue with a Domain Name

BC 8	Help a certification authority determine and validate the identity of the entity associated with a domain name that will be bound to an SSL/TLS certificate
BC 9	Search Engines, Messaging Services & Social Media Platforms seeking to confirm the authenticity of businesses advertising or Posting News on its Platform
ALAC 1	Online buyers identifying and validating the source of goods or services/ Internet users validating the legitimacy of an email or a website to protect themselves
ALAC 2	Consumer protection organizations